Andriesei C.
5403

LUMINIŢA SCRIPCARIU
IULIAN-DRAGOŞ SCRIPCARIU

REŢELE DE CALCULATOARE

TEHNOPRESS
IAŞI – 2003

Referenţi ştiinţifici:

Prof. dr. ing. **Petruţ DUMA**
Universitatea Tehnică „Gh.Asachi" Iaşi

Prof. dr. ing. **Daniela TĂRNICERIU**
Universitatea Tehnică „Gh.Asachi" Iaşi

EDITURA TEHNOPRESS
Str. Zimbrului nr.17
700047 Iaşi
Tel./fax: 0232 260092
E-mail: tehnopress@k.ro

Editura Tehnopress Iaşi este acreditată C.N.S.I.S

Descrierea CIP a Bibliotecii Naţionale a României
SCRIPCARIU, LUMINIŢA
Reţele de calculatoare/ Luminiţa Scripcariu, Iulian-Dragoş Scripcariu – Iaşi: Tehnopress, 2003
250 p.; 24 cm.
Bibliogr.
ISBN 973-8377-12-9
I. Scripcariu, Iulian-Dragoş

621

ISBN 973-8377-12-9

PREFAŢĂ

Volumul de faţă prezintă principiile şi elementele fundamentale, dar şi o serie de concepte complexe ale reţelelor de calculatoare locale şi ale celor de arie largă, ale protocoalelor de comunicaţii şi serviciilor de reţea.

Cartea este structurată în trei părţi, realizând o tratare graduală a problematicii reţelelor de calculatoare.

Prima parte, cuprinzând capitolele I, II, III şi IV, este dedicată modelelor de reţea (OSI, TCP/IP, client-server), suitelor de protocoale de comunicaţii (TCP/IP, IPX/SPX, ATM), standardelor de reţele locale (Ethernet, Fast Ethernet, GigaEthernet, Token-Bus, Token-Ring, FDDI, IsoEthernet,WLAN) şi echipamentelor specifice reţelelor locale (cabluri, interfeţe, hub-uri, switch-uri). Anexa A prezintă algoritmii de reţea într-un mod aplicativ, care permite înţelegerea funcţionării diferitelor tipuri de reţele, a metodelor de acces la mediu şi a celor de soluţionare a problemelor de trafic (coliziuni, congestii).

Cea de a doua parte, respectiv capitolul V, tratează relativ succint sistemele de operare de reţea şi driverele pentru plăcile de reţea. În completare, anexa B prezintă o serie de comenzi specifice sistemului UNIX, prin care cititorul se familiarizează cu sistemul de fişiere şi modul de lucru sub UNIX.

În partea a treia a cărţii, reprezentată de ultimele două capitole, sunt descrise reţelele de arie largă, echipamentele de interconectare a reţelelor locale (bridge, router, firewall), precum şi diferite servicii, protocoale şi standarde specifice WAN (Frame Relay, VLAN, ISDN, VoP, X.25, TDM, PPP, xDSL).

Sunt indicate referinţe bibliografice utile, documentele RFC specificate pe parcursul expunerii fiind disponibile pe *web* (WWW).

Referitor la adresarea IP, sunt propuse o serie de aplicaţii pentru aprofundarea modului de adresare în reţele şi a celui de definire a subreţelelor.

Lista de abrevieri este deosebit de utilă pentru urmărirea uşoară a materialului şi învăţarea terminologiei specifice reţelelor.

Numeroase exemple sunt date pentru aprofundarea conceptelor prezentate și înțelegerea modalităților de configurare a echipamentelor de rețea. Evident este necesară efectuarea unor lucrări practice pentru cunoașterea în detaliu a echipamentelor. De asemenea, este utilă consultarea documentațiilor tehnice oferite de firmele producătoare care prezintă aspectele particulare ale fiecărui echipament de rețea.

În ansamblu, această carte se adresează atât studenților, cât și specialiștilor din domeniul rețelelor de calculatoare.

AUTORII

CUPRINS

Capitolul I. NOȚIUNI DE BAZĂ PRIVIND REȚELELE DE CALCULATOARE

I.1 Introducere 9
I.2 Modelul de rețea stratificată ISO/OSI 14
I.3 Modelul TCP/IP 20
I.4 Arhitectura rețelelor de comunicații 22
I.4.1 Modul de acces la mediul fizic de transmisie 22
I.4.2 Topologia logică 23
I.4.3 Topologia fizică 23

Capitolul II. PROTOCOALE DE COMUNICAȚII

II.1 Suita de protocoale TCP/IP 27
II.1.1 Protocolul INTERNET. Adresarea IP 32
II.1.2 DNS - Sistemul numelor de domenii Internet 39
II.1.3 Protocoale de adresare (ARP, RARP, BOOTP, DHCP) 41
II.1.4 Protocoale de transport (TCP, UDP) 45
II.1.5 Protocolul Telnet 49
II.1.6 Protocolul Finger 51
II.1.7 Protocoale de poștă electronică (SMTP, POP) 52
II.1.8 Protocoale pentru transferul fișierelor (FTP, TFTP, SFTP) 58
II.1.9 Protocoale de timp pentru Internet 64
II.1.10 Protocolul ICMP 66
II.1.11 Protocoale de management a rețelei 68
II.1.12 Protocoale de securitate în Internet 73
II.2 Suita de protocoale Novell IPX/SPX 77
II.3 Suita de protocoale ATM 80

Capitolul III. STANDARDE DE REȚELE LOCALE

III.1 Standarde ETHERNET. Standardul IEEE 802.3 84
III.2 Standardul IEEE 802.4. Rețea Token-Bus 88

III.3 Standardul IEEE 802.5. Rețea Token-Ring 90
III.4 FDDI 94
III.5 ISO-ETHERNET 96
III.6 Standardul IEEE 802.11. Rețea WLAN 97
III.7 Analiza standardelor pe baza modelului OSI 99

Capitolul IV. ECHIPAMENTE DE COMUNICAȚII PENTRU LAN

IV.1 Cabluri de transmisie 100
IV.2 Interfețe de comunicație 105
IV.3 Repetoare multiport (Hub) 111
IV.4 Comutatoare de rețea (Switch) 114
IV.5 Modemuri 118

Capitolul V. SISTEME DE OPERARE

V.1 Generalități privind sistemele de operare 131
V.2 Tipuri de sisteme de operare 134
V.3 Modelul structurat al unui sistem de operare de rețea 137
V.4 Tipuri de drivere pentru plăcile de rețea 140
V.5 Windows NT 143
V.5.1 Domenii NT 145
V.5.2 Servicii NT 148
V.6 UNIX 150

Capitolul VI. INTERCONECTAREA REȚELELOR LOCALE

VI.1 Punți de rețea (Bridge) 154
VI.2 Echipamente de dirijare (Router) 159
VI.3 Protocoale de rutare 162
VI.3.1 Protocoale de rutare cu vectori de distanță 164
VI.3.2 Protocoale de rutare bazate pe starea legăturii 164
VI.3.3 Rutarea IP 165
VI.4 Rețele locale virtuale (VLAN) 168
VI.5 Echipamente de securizare (Firewall) 175

CAPITOLUL VII. SERVICII ȘI TEHNOLOGII WAN

VII.1 Schimbul de cadre (FRAME RELAY) 179
VII.1.1 Încapsularea Frame Relay 180
VII.1.2 Identificarea conexiunilor Frame Relay 182
VII.1.3 Gestionarea rețelelor Frame Relay 182
VII.1.4 Interfețe Frame Relay 184
VII.1.5 Congestia rețelelor Frame Relay 184
VII.2 Transmisia vocii în pachete (VoP) 187
VII.2.1 Interoperabilitatea serviciului VoP 187
VII.2.2 Calitatea serviciului de voce 189
VII.2.3 Arhitectura sistemului VoIP 190
VII.2.4 Caracteristicile serviciului VoATM 191
VII.2.5 Echipamente de transmisie VoP 192
VII.3 ISDN 193
VII.3.1 Interfețe BRI 194
VII.3.2 Interfețe PRI 195
VII.3.3 LAPD 198
VII. 3.4 AODI 199
VII.4 X.25 200
VII.4.1 LAPB 202
VII.4.2 Încapsularea datelor în rețeaua X.25 202
VII.5 TDM 203
VII.6 PPP 206
VII.6.1 Încapsularea datelor prin PPP 206
VII.6.2 Protocoale de control 208
VII.6.3 Modalități de alocare a benzii 208
VII.6.4 Legături PPP prin modemuri telefonice 209
VII.7 Tehnologii xDSL 210

ANEXA A. ALGORITMI DE REȚEA 213
A.1 Algoritmul nodului *master* 214
A.2 Algoritmul unui nod *slave* 216
A.3 Algoritmul unui nod dintr-o rețea descentralizată 216
A.4 Algoritmul CSMA/CD 218

A.5 Algoritmul Token-Bus 220
A.6 Algoritmul Token-Ring 221

ANEXA B. COMENZI UNIX UZUALE 225
B.1 Generalități 225
B.2 Organizarea sistemului de fișiere sub UNIX 228
B.3 Comenzi de operare cu directoarele 229
B.4 Comenzi de operare cu fișierele 232

ABREVIERI 237
BIBLIOGRAFIE 249

I

NOȚIUNI DE BAZĂ PRIVIND REȚELELE DE CALCULATOARE

I.1 INTRODUCERE

Utilitatea calculatorului este de necontestat în toate domeniile de activitate. În plus, interconectarea calculatoarelor devine necesară pentru realizarea comunicației dintre utilizatori.

Accesul la paginile *web* ale diferitelor persoane, firme și instituții ori la bazele de date publice sau private reprezintă un beneficiu pentru obținerea într-un mod comod și rapid a informațiilor dorite. Prin realizarea unei rețele de calculatoare (*internet*) se împart (*sharing*) fie resursele informaționale (*software*), fie cele fizice (*hardware*).

Internet-ul este cea mai largă colecție de rețele de calculatoare din lume, care cuprinde toate rețelele naționale și regionale de pe glob.

Dacă se interconectează calculatoarele dintr-o încăpere, clădire sau campus astfel încât distanța maximă dintre procesoare să nu depășească câțiva kilometri, atunci se formează o **rețea locală** (*LAN-Local Area Network*).

La nivelul unei localități, cu dimensiuni de ordinul zecilor de kilometri, prin interconectarea mai multor LAN-uri, se obține o **rețea metropolitană** (*MAN-Metropolitan Area Network*).

La nivelul unei țări sau chiar continent, acolo unde distanțele maxime dintre procesoare sunt de ordinul sutelor sau miilor de kilometri, se implementează **rețele de arie largă** (*WAN-Wide Area Network*).

Observație: În mod uzual se face abstracție de distanța maximă dintre procesoare și se spune că prin interconectarea mai multor LAN-uri se obține un WAN.

Printr-o rețea locală sunt interconectate mai multe calculatoare-gazdă (*host*) și unul sau mai multe servere.

Termenul de *World Wide Web*, abreviat **WWW**, semnifică o rețea de calculatoare extinsă la nivel mondial. Sugestiv este faptul că, printre altele, cuvântul *web* înseamnă și "pânză de păianjen".

Mai precis, WWW sau W3 este un sistem informațional distribuit, bazat pe o arhitectură de tipul client-server. O aplicație de tip client Web adresează o cerere unui server Web care la rândul său răspunde fie prin transferul unor fișiere (de tip text, imagine, audio, video etc) de la server la client, fie realizează hiperlegături spre alte surse de informații (*hyperlink*).

Un utilizator conectat la Internet de oriunde în lume are acces la informație, ignorând distanțele și economisind timp și bani, doar dacă știe adresa respectivei surse de informație sau pagini web. WWW tinde să devină o bază de date universală.

Prin **URL** (*URL - Uniform Resource Locator*) înțelegem un format standard care specifică numele, tipul și locația documentelor sau surselor de informație dintr-o rețea. Scopul URL constă în încapsularea informațiilor necesare unui program de rețea pentru localizarea unui obiect în Internet. El acționează ca o adresă de rețea și identifică inclusiv metoda de acces spre obiectul respectiv.

Sintaxa generică URL este: `tip://gazda.domeniu[:port]/cale/nume`.

Prin `tip` se specifică protocolul utilizat pentru comunicație. De exemplu, pe un server WWW se folosește tipul `http` (HTTP - *HyperText Transfer Protocol*), pe un server FTP (*File Transfer Protocol*) se specifică `ftp` iar în cazul unei cereri Telnet se specifică tipul `telnet`.

Exemplu: `http://www.etc.tuiasi.ro`.

Domeniul este declarat în Internet prin **DNS** (*Domain Name System*), un mecanism de asociere a numelor diferitelor locații (*site*-uri) cu adresele IP (*Internet Protocol*) numerice de 32 de biți (4 octeți exprimați în format zecimal cu puncte) ale calculatoarelor-gazdă din rețelele bazate pe suita de protocoale TCP/IP (*Transmission Control Protocol/Internet Protocol*). Mai exact, adresa IP respectivă este atribuită plăcii de rețea (NIC - *Network Interface Card*) cunoscându-se adresa MAC (*Media Access Control*) a acesteia, exprimată prin 6 octeți în format hexazecimal și alocată în mod unic de către producător.

Exemple: adresă IP 193.226.26.14; adresă MAC: 2C-03-E1-42-0F-A5.

DNS împarte fiecare domeniu din Internet în subdomenii, structurate ierarhic ca într-o diagramă de tip 'arbore'. Fiecare domeniu este denumit de calea în arbore până la nodul-rădăcină, componentele fiind separate prin puncte. O componentă are cel mult 64 de caractere, iar lungimea întregii căi nu depășește 255 de caractere.

Domeniile pot fi inserate în 'arbore' fie pe criteriul **geografic** (de exemplu, `ro` - este indicativul de țară pentru România; pentru alte țări se folosesc indicativele geografice ale acestora, cum sunt: `us,ca,uk,fr,jp`), fie pe criteriul **generic** (`com` - comercial, `edu` - educațional, `gov` - guvernamental, `int` - internațional, `mil` - militar, `org` - organizații nonprofit, `net` - rețele de ccomunicații). Căutarea adresei IP a unei destinații se face prin interogarea iterativă, recursivă sau nerecursivă, a serverelor de nume (*name server*), responsabile de anumite zone din Internet.

Indiferent care sunt firmele producătoare de calculatoare și de echipamente de comunicații, rețeaua de comunicații trebuie să asigure legătura între toți utilizatorii. Astfel a apărut conceptul de **sistem deschis** (*Open System*) care poate interconecta echipamentele produse în diferite tehnologii, de diverși producători, pe baza **modelului de rețea OSI** (*Open Systems Interconnection*) cu suita de protocoale specificată prin standarde ISO (*International Organisation for Standardisation*).

În general, prin **protocol** se înțelege o suită de reguli și formate impuse pentru reprezentarea datelor și transferul lor între două sau mai multe calculatoare.

Transmisia informației se realizează prin diferite medii fizice de transmisie (conductor metalic în cablu torsadat sau coaxial, fibră optică , eter).

Pentru transmisii de date la mare distanță, pe linie telefonică sau prin undă radio pentru comunicații 'fără fir' (*wireless*), se impune utilizarea unor **modem**-uri (DCE - *Data Communication Equipment*) care să convertească șirul de biți generat de calculator în semnal analogic modulat adaptat benzii de transmisie a canalului de comunicații.

Controlul comunicației dintre terminalele sau calculatoarele dintr-o rețea (DTE - *Data Terminal Equipment*) se realizează prin intermediul echipamentelor de comunicație (interfață, *hub, switch, bridge, firewall, gateway* sau *router*) și al serverelor, care dispun de puternice resurse hardware și software (Fig.I.1).

În figură, este reprezentată o rețea locală de calculatoare cu două subrețele A și B care deservesc două departamente. Fiecare hub asigură accesul multiplu al utilizatorilor dintr-o subrețea la un canal de transmisie reprezentat de cablul de legătură dintre switch și hub. Evident se poate extinde rețeaua în funcție de numărul de porturi cu care este prevăzut switch-ul.

Calculatorul server este conectat direct în switch astfel că viteza de transmisie a datelor înspre și dinspre server este maximă.

Imprimanta de rețea poate fi activată de la distanță de către oricare utilizator din rețea.

Integrarea acestei rețele locale într-una de arie extinsă se face prin intermediul router-ului, care în particular poate funcționa ca "zid de protecție" (*firewall*).

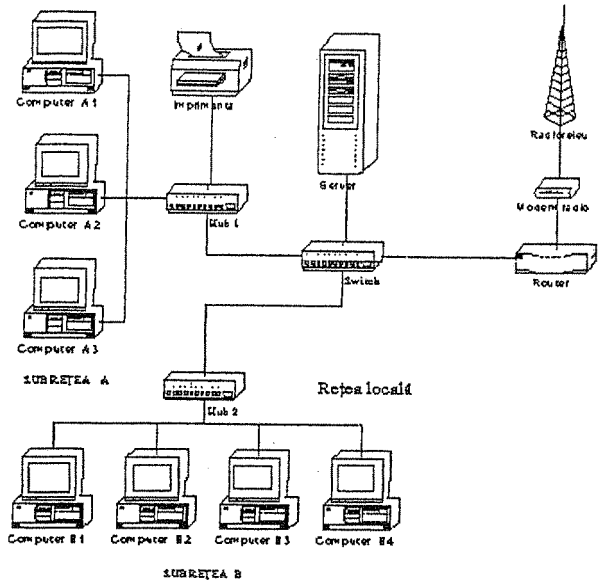


Fig.I.1. Exemplu de rețea locală cu legătură la distanță pe linie de radioreleu

Legătura la distanță cu alte rețele locale se poate implementa fie pe cablu, fie în eter prin undă radio. În particular, s-a considerat o legătură la distanță 'fără fir'. Modem-ul extern este necesar doar dacă nu se folosește un router radio.

Un radioreleu de mică capacitate amplasat corespunzător (la înălțime, pe o clădire sau pe un pilon), va asigura conexiunea cu un alt nod al rețelei WAN.

Observații:

1. Se preferă adoptarea și utilizarea directă a termenilor din limba engleză întrucât achiziționarea echipamentelor se face de obicei cu documentația tehnică oferită de firma producătoare, redactată într-una din limbile de largă circulație, dintre care nu lipsește cea engleză.
2. Includerea unui LAN într-un WAN se face prin intermediul routerului, acesta nefiind considerat o componentă a LAN-ului.
3. O rețea de calculatoare poate fi reprezentată grafic sub formă de graf. Nodurile terminale corespund DTE-urilor iar cele intermediare DCE-urilor. Arcurile, orientate sau neorientate, dintre noduri reprezintă legăturile fizice dintre echipamente. Metoda este utilă pentru aplicarea eficientă a algoritmilor de rutare, bazați pe metoda deducerii "drumului minim" dintr-un graf (STA - *Spanning Tree Algorithm*).

Securitatea rețelelor de comunicație privind integritatea datelor stocate în rețea și restricționarea accesului persoanelor neautorizate este o problemă stringentă în condițiile în care tot mai multe atacuri apar pe Internet, dar și în rețelele locale și regionale. O altă problemă acută a rețelelor o constituie asigurarea fluenței traficului informațional și evitarea **congestiilor** (blocaje de trafic). În principal, aceste probleme se soluționează prin configurarea adecvată a echipamentelor de comunicație (*server, bridge, router*) din rețea. La nivelul așa-numitului *firewall* sau "zid de foc (de protecție)", echipament care stabilește limite privind comunicația dintre două sau mai multe rețele, este posibil controlul accesului unităților de date prin filtrarea **pachetelor** (*packets filtering*), al utilizatorilor prin autentificare (*authentication*) pe baza unor parole (*password; passphrase*), eventual și al drepturilor de accesare a anumitor aplicații prin includerea unor porți de aplicație (*gateways*).

Se pot utiliza metode combinate de compresie și criptare (ENCO - *ENcryption & COmpression*) ori cartele de acces cu suport magnetic sau optic (MAC - *MiniAccelerator Card*), pentru criptarea și decriptarea datelor, limitând hardware accesul la informație al diferiților utilizatori. Pentru confidențialitatea mesajelor transmise prin poșta electronică se poate utiliza schema de criptare PGP (*Pretty Good Privacy*).

Prin adoptarea unor algoritmi software bazați pe protocoale specifice de control a comunicației și rutare a datelor, se realizează controlul traficului informațional (drept de acces, viteză de transmisie, lățime de bandă alocată etc) și se pot evita și soluționa eventualele congestii din rețea.

APLICAȚII

1. Încărcați de pe Internet documentul RFC 1738, *Uniform Resource Locator (URL),* autori Berners-Lee, Masinter și McHill (1994) și studiați caracteristicile de bază ale URL. Realizați eventual transferul fișierului de pe site-ul `www.w3.org`. Căutați documente RFC referitoare la URI (*Uniform Resource Identifier*). Ce legături există între URI, URL și URN?

2. Referitor la metoda PGP, încărcați de pe Internet și studiați documentul `pgpfaq?.asc`, accesibil prin FTP anonim la `/pub/gb/gbe`, pe site-ul `ftp.netcom.com`. Se pot accesa și informațiile despre PGP, disponibile la grupul de știri din Internet `alt.security.pgp`.

I.2 MODELUL DE REȚEA STRATIFICATĂ ISO/OSI

Proiectarea, întreținerea și administrarea rețelelor de comunicații se poate face mai eficient dacă se au în vedere obiectivele de utilizare a acestora.

De multe ori, cercetările efectuate în acest domeniu nu au avut un efect substanțial asupra performanțelor și eficienței de utilizare a rețelelor de comunicații. Acest fapt este cunoscut sub numele de **paradoxul productivității**, adică unele progrese tehnologice mari nu determină o creștere considerabilă a productivității sistemului. De aceea, pentru analiza și proiectarea rețelelor de comunicații, trebuie avut în vedere **modelul sus-jos** (*Top-Down Model*) prezentat în figura I.2, bazat pe principiul că o rețea oferă soluții care trebuie să satisfacă cerințele clientului.

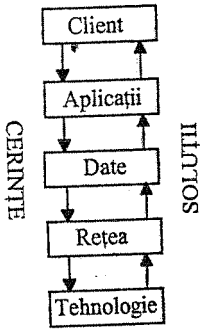


Fig. I.2 Modelul 'sus-jos'

În funcție de activitatea desfășurată, clientul solicită o anumită aplicație care poate fi rulată într-o rețea de calculatoare. Se strâng apoi informații despre natura datelor care vor fi vehiculate. Termenul generic de **date** semnifică, pe lângă șirul de biți generat de un terminal de date, reprezentarea în format digital binar a semnalelor (voce, audio, video, imagini fixe etc). Natura datelor este esențială în alegerea unui anumit mediu fizic de transmisie, precum și a arhitecturii rețelei. Suplimentar însă, modul de implementare a rețelei va depinde și de costurile maxim admise, ceea ce va impune alegerea unei anumite variante tehnologice (*hardware*). Astfel se deduce soluția optimă care corespunde cerințelor clientului.

Pornind de la acest model, pe principiul stratificării, ISO a propus modelul stratificat OSI de interconectare a echipamentelor produse de diverse firme, pentru realizarea sistemelor deschise de comunicație.

Modelul OSI (*Open Systems Interconnection*) prevede șapte nivele (*layers*), în care mediul fizic de transmisie nu este inclus (Fig.I.3). Acestor nivele li se asociază un set de protocoale specifice, denumite **protocoale OSI**, care nu sunt incluse în modelul OSI.

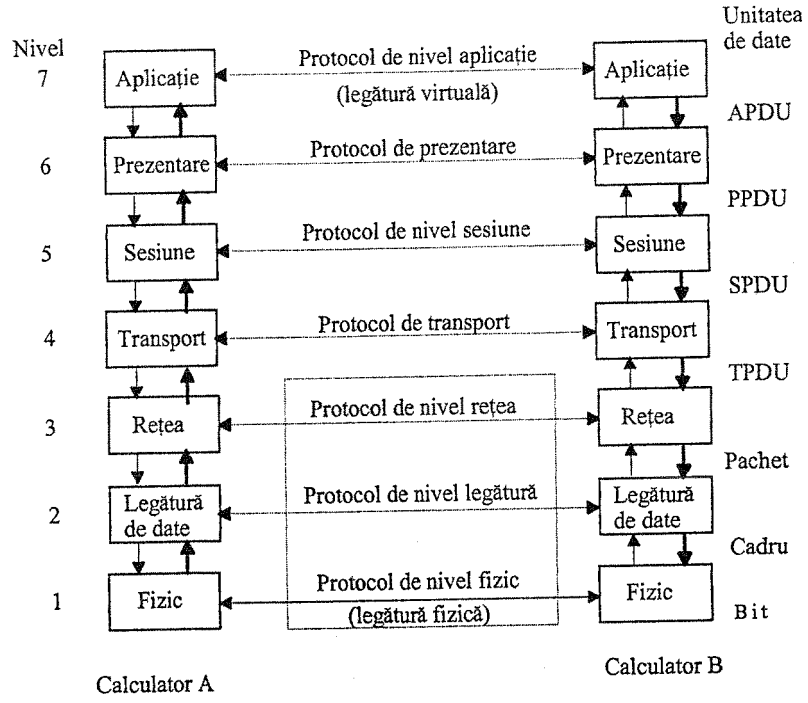


Fig. I.3 Modelul de rețea OSI și suita de protocoale OSI

În figura I.3, calculatoarele A și B sunt reprezentate pe baza modelului OSI. Transferul datelor de la A la B, respectiv de la B la A, se face pe traseele marcate cu linie continuă, subțire și îngroșată. Datele sunt transmise între echipamente prin legătura fizică.

Între nivelele similare ale terminalelor, comunicația se realizează pe baza unui protocol specific, denumit după numele nivelului. Cu excepția protocolului de la nivelul fizic, toate celelalte sunt asociate unor **comunicații virtuale prin legăturile virtuale** (*virtual path*) deoarece nu există o legătură reală între nivelele respective, datele transferându-se doar la nivel fizic, acolo unde are loc **comunicația reală (fizică)** dintre calculatoare, printr-un **circuit fizic.**

Dacă cele două calculatoare nu aparțin aceleiași rețele, atunci protocoalele de nivele 1, 2 și 3 se aplică prin intermediul echipamentelor de comunicație care interconectează rețelele (*switch, bridge, router* sau *gateway*), în așa-numita **subrețea de comunicație** (*subnetwork*).

Se observă că pe fiecare nivel se denumește altfel unitatea de date (DU - *Data Unit*).

Denumirea unității de date pe fiecare nivel al modelului OSI depinde de protocolul aplicat. În figura I. 3, s-au folosit pentru nivelele superioare, termeni generici cum ar fi APDU (*Application Protocol Data Unit*), PPDU (*Presentation Protocol DU*), SPDU (*Session Protocol DU*), TPDU (*Transport Protocol DU*) care vor căpăta denumiri specifice funcție de suita de protocoale folosită într-o anumită rețea. De exemplu, în protocoalele TCP/IP se folosesc termenii de **datagramă, mesaj, segment.** Pe nivel fizic datele sunt transmise sub formă de **biți**. Pe nivelul legăturii de date se transferă **cadre de date** (*frame*), iar la nivelul de rețea se folosește termenul consacrat de **pachet** (*packet*).

La **nivelul aplicație** se implementează algoritmii software care convertesc mesajele în formatul acceptat de un anumit terminal de date real. Transmisia se realizează în formatul standard specific rețelei. Față de aceste standarde de comunicație, DTE-ul real devine un **terminal virtual** care acceptă standarde de rețea specifice (de exemplu VT100/ANSI).

Nivelul de prezentare se ocupă de respectarea sintaxei și semanticei impuse de sistem, de codificarea datelor (compresie, criptare) și reprezentarea lor în formatul standard acceptat. În plus, acest nivel supervizează comunicațiile în rețea cu imprimantele, monitoarele, precum și formatele în care se transferă fișierele.

Nivelul de sesiune furnizează diverse servicii între procesele-pereche din diferite noduri: transfer de fișiere, legături la distanță în sisteme cu acces multiplu, gestiunea jetonului (*token*) de acordare a permisiunii de a transmite date, sincronizarea sistemului etc. O sesiune începe doar dacă legătura între noduri este stabilită, deci este orientată pe conexiune. Nivelul sesiune este considerat ca fiind interfața dintre utilizator și rețea.

Nivelul de transport deplasează datele între aplicații. Acest nivel răspunde de siguranța transferului datelor de la sursă la destinație, controlul traficului, multiplexarea și demultiplexarea fluxurilor, stabilirea și anularea conexiunilor din rețea. De asemenea, la acest nivel mesajele de mari dimensiuni pot fi **fragmentate** în unități mai mici, **pachete**, cu lungime impusă, procesate și transmise independent unul de altul. La destinație, același nivel răspunde de refacerea corectă a mesajului prin ordonarea pachetelor indiferent de căile pe care au fost transmise și ordinea sosirii acestora.

Pe **nivelul de rețea**, se alege calea de expediere a pachetului, se realizează controlul traficului informațional din rețea si dintre rețele, se rezolvă congestiile, eventual se convertește formatul pachetului dintr-un protocol în altul. În unele LAN-uri, funcția nivelului de rețea se reduce la cea de stocare (*buffering*) și retransmisie a pachetelor. În WAN-uri, la acest nivel se realizează operația de **rutare** a pachetelor, adică stabilirea căilor optime de transmisie între noduri.

La **nivelul legăturii de date** circulă **cadre** de biți, adică pachete împachetate sau încapsulate, cu antet (H - *header*) și marcaj final (T - *trail*), care includ adresele sursei (SA - *Source Address*) și destinației (DA - *Destination Address*) pentru a se putea expedia datele între calculatoare. Suplimentar, în cadrul de date sunt incluse: un câmp de control al erorilor, unul responsabil de sincronizarea transmisiei, un câmp de protocol etc.

În principal, nivelul legăturii de date este responsabil de detecția erorilor de transmisie a datelor prin rețea. În Internet, se utilizează **sume de control** (*check sum*), calculate la emisie și la recepție, prin sumarea în GF(*Galois Field*) a tuturor blocurilor de 16 biți din câmpul datelor (RFC 1071). Aceste sume permit detecția erorilor simple, eventual a unor erori multiple. În alte cazuri, se folosesc **coduri ciclice** (CRC - *Cyclic Redundancy Code*) care au o capacitate mai mare de detecție a erorilor decât sumele de control. Pentru aplicații speciale se codifică datele în baza unei tehnici de codare pentru corecția erorilor de transmisie (Hamming, Reed-Solomon etc), ceea ce permite eliminarea retransmisiilor de cadre și creșterea eficienței canalului de comunicație.

Nivelul legăturii de date este împărțit în două subnivele: LLC (*Logical Link Control*) și MAC (*Media Access Control*) (Fig. I.4). Aceste subnivele stabilesc modalitățile de acces la mediu în cazul canalelor de comunicație cu acces multiplu și realizează controlul traficului pentru a se evita efectele neadaptării ratelor de transmisie ale echipamentelor și posibilitatea saturării lor (*flooding*).

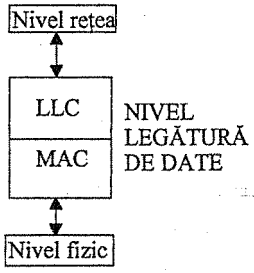


Fig. I.4 Subnivelele de nivel 2
și interconectarea cu nivelele adiacente din modelul OSI

La **nivel fizic**, se transmit datele în format binar (biți 0 și 1) pe canalul de comunicație din rețea. În standardele echipamentelor care lucrează la nivel fizic, precum și în cele ale interfețelor fizice aferente acestora, sunt specificate caracteristicile lor electrice, mecanice, funcționale și procedurale. Natura sursei de informație (date, voce, audio, video) nu se mai cunoaște la acest nivel ceea ce face ca procesul de comunicație să fie considerat transparent.

Fiecare nivel are rolul de a ascunde nivelului superior detaliile de transmisie către nivelul inferior și invers. Nivelele superioare beneficiază de serviciile oferite de cele inferioare în **mod transparent.** De exemplu, între nivelele-aplicație informația circulă fără erori (*error-free*) deși apar erori de transmisie pe canalul de comunicație, la nivel fizic, detectate și corectate la nivelul legăturii de date.

Nivelele modelului OSI pot fi implementate fizic (*hardware*) sau logic (*software*). Evident nivelul fizic este implementat fizic (interfețe fizice, conectori de legătură). Nivelul legăturii de date poate fi implementat logic dar se preferă varianta fizică, aceasta asigurând viteze mari de procesare. Nivelele superioare sunt de obicei implementate logic, ca procese, în cadrul sistemului de operare sau separat, dar activate de acesta.

Orice nivel lucrează pe principiul modelului I-P-O (*Input - Processing - Output*), adică dacă se cunosc formatul semnalului sau secvenței de intrare și cerințele pentru generarea ieșirii, protocolul de pe nivelul respectiv are rolul de a procesa intrarea pentru a se face adaptarea cu nivelul următor. Afirmația este valabilă în ambele sensuri de transmisie în nivelul OSI (sus-jos și jos-sus).

Conectarea terminalului de date la mediul fizic de transmisie se realizează prin intermediul **interfeței fizice** cu caracteristicile specificate de nivelul fizic.

Exemple: RS - 232 C(D), RS - 485, X.21, X.25, V.35.

Între nivelele superioare se intercalează interfețe implementate doar prin soft și denumite **interfețe logice.** De exemplu, în sistemele cu multiplexare în timp, cum ar fi sistemele de transmisie sincrone (SDH - *Synchronous Digital Hierarchy)*, un canal E1 cu 30 de canale PCM (*Pulse Code Modulation*) trebuie partajat pentru asigurarea accesului multiplu.Utilizatorilor li se alocă anumite intervale de transmisie (*time slot*), pe baza protocolului de legătură punct-la-punct (PPP - *Point-to-Point Protocol*) prin interfețele logice *ppp.*

Modelul OSI este foarte general, pur teoretic, și asigură o mare flexibilitate în cazul dezvoltării rețelelor prin separarea diverselor funcții ale sistemului pe nivele specifice. Numărul relativ mare de nivele din acest model face necesară utilizarea unui mare număr de interfețe și a unui volum crescut de secvențe de control. De aceea, în numeroase cazuri se va folosi un număr redus de nivele. Modelul OSI nu constituie un standard ci doar o referință pentru proiectanții și utilizatorii de rețele de calculatoare.

Un model interesant este acela care separă nivelul-aplicație, mai precis procesorul de aplicații (AP - *Application Processor*) de cel care realizează efectiv comunicația, așa-numitul **procesor de comunicație** (CP - *Communication Processor*) și de mediul fizic de transmisie (*Communication Link*). Se obține un model cu trei straturi între care se intercalează interfețele de

transmisie (Fig. I.5). Evident, comunicația directă între nivelele-aplicație este una virtuală. Acestea comunică real prin intermediul straturilor inferioare.

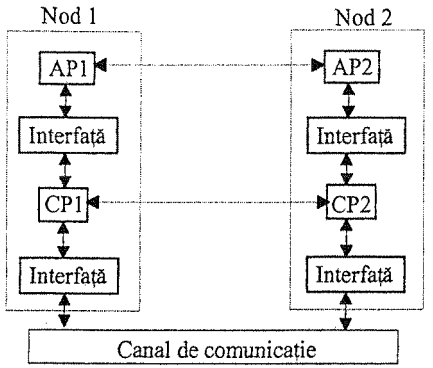


Fig. I.5 Model de rețea de comunicație cu trei nivele

Deosebit de util pentru înțelegerea proceselor de comunicații dintre aplicații și realizarea programelor de aplicații pentru rețea este **modelul client-server.**

Clientul este partea hardware sau software care adresează o cerere (de acces, de informare, de transfer de fișiere etc). **Serverul** este partea hardware sau software care răspunde cererii clientului (Fig. I.6).

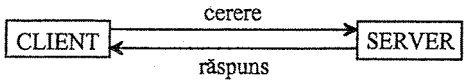


Fig. I.6 Modelul client-server

Aplicația server se autoinițializează după care rămâne într-o stare de așteptare până la primirea unei cereri de serviciu de la un proces client. Aplicația client este cea care solicită a conexiune iar aplicația server primește cererea și o rezolvă. Între cele două aplicații apare o conversație virtuală ca și cum între ele ar exista o conexiune punct-la-punct.

I.3 MODELUL TCP/IP

Familia de protocoale în baza căreia se realizează comunicația în rețelele eterogene de calculatoare conectate la Internet este denumită **suita de protocoale Internet** sau, mai simplu, TCP/IP (*Transmission Control Protocol/Internet Protocol*). De asemenea, termenul de **tehnologie Internet** semnifică suita de protocoale TCP/IP și aplicațiile care le folosesc (RFC 1180). Suita de protocoale TCP/IP gestionează toate datele care circulă prin Internet.

Modelul suitei de protocoale TCP/IP are patru nivele, care corespund modelului OSI până la nivelul de transport.

Modelul stratificat de protocoale TCP/IP este diferit de modelul OSI (*Open System Interconnection*), dar se pot face echivalări între acestea (Fig.I.7). TCP/IP împreună cu modelul NFS (*Network File System*) acoperă funcțiile tuturor nivelelor OSI. Cele două familii de protocoale (TCP/IP și NFS) alcătuiesc așa-numitul context de operare a rețelelor deschise (ONC - *Open Network Computing*).

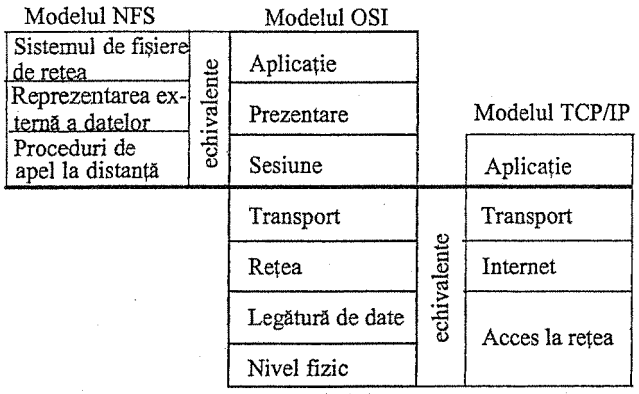


Fig.I.7 Modelul TCP/IP și echivalențele dintre modelele de rețea (OSI, NFS, TCP/IP)

TCP și IP sunt doar două protocoale din această suită. Stiva de protocoale TCP/IP include mai multe protocoale, pe diferite nivele ale modelului (Fig. I.8):

PPP - *Point -to-Point Protocol;*

SLIP - Serial Line Internet Protocol;

ARP - *Address Resolution Protocol;*

RARP - *Reverse Address Resolution Protocol;*

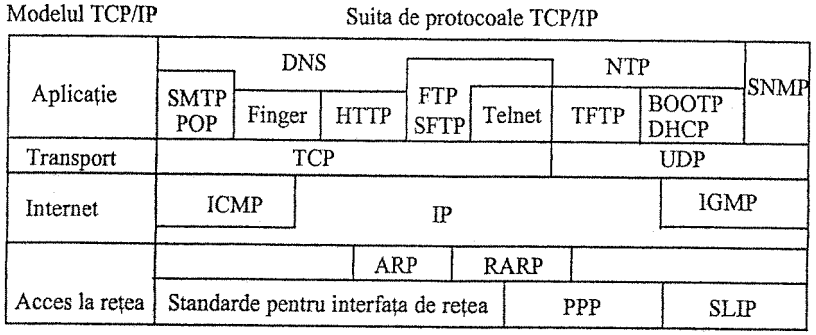


Fig. I.8 Stiva de protocoale TCP/IP

IP - *Internet Protocol;*

ICMP - *Internet Control Message Protocol;*

IGMP - *Internet Group Management Protocol;*

TCP - *Transport Control Protocol;*

UDP - *User Datagram Protocol;*

DNS - *Domain Name System;*

NTP - *Network Time Protocol;*

SMTP - *Simple Mail Transfer Protocol;*

POP - *Post-Office Protocol;*

Finger - *Finger User-information Protocol;*

FTP - *File Transfer Protocol;*

SFTP- *Simple File Transfer Protocol;*

Telnet - *Virtual Terminal Connection;*

TFTP - *Trivial File Transfer Protocol;*

BOOTP - *BOOTstrap Protocol;*

DHCP - *Dynamic Host Configuration Protocol;*

SNMP - *Simple Network Management Protocol.*

Protocoalele de aplicație colaborează cu protocoalele de pe nivelele inferioare ale stivei TCP/IP pentru a transmite date prin Internet, mai precis pentru a oferi servicii utilizatorului (poștă electronică, transfer de fișiere, acces în rețea de la distanță , informații despre utilizatori etc), prin intermediul programelor de aplicații care implementează diverse protocoale (POP, FTP, Telnet, Finger etc).

I.4 ARHITECTURA REȚELELOR DE COMUNICAȚII

Pentru descrierea arhitecturii unei rețele de calculatoare trebuie precizate modalitatea de acces la mediu, topologia logică și topologia fizică a acesteia.

Alegerea mediului de transmisie și a unei arhitecturi specifice reprezintă operația de **configurare** a rețelei.

Rețelele de calculatoare se pot implementa fizic fie ca **rețele cu difuzare** (PMP - *Point - to - Multipoint*), fie ca **rețele punct-la-punct** (PP - *Point-to-Point*).

În cadrul unei **rețele cu difuzare,** toate calculatoarele sunt conectate la un singur canal de transmisie cu acces multiplu (*Multiple Access Channel*), multiplexarea făcându-se static sau dinamic:

1. în frecvență (FDMA - *Frequency Division Multiple Access*);
2. în timp (TDMA - *Time Division Multiple Access*);
3. în cod (CDMA - *Code Division Multiple Access*);
4. în lungime de undă (WDMA - *Wavelength Division Multiple Access*).

Într-o astfel de rețea, un mesaj sau pachet de date poate fi transmis unui singur terminal (*unicast*), sau către un grup predefinit de utilizatori (*multicast*) sau către toate calculatoarele din rețea (*broadcast*).

Într-o rețea de tip **"punct-la-punct"**, există conexiuni multiple între terminale (**noduri**) astfel că un pachet poate fi transmis la destinație pe mai multe căi, fiind necesară implementarea unor algoritmi de dirijare sau rutare a pachetelor.

De obicei, rețelele locale sunt "cu difuzare", iar cele WAN sunt "punct-la-punct".

I.4.1 Modul de acces la mediul fizic de transmisie

Într-o rețea cu difuzare este posibil ca mai mulți utilizatori să transmită date în același timp. Dacă aceștia sunt conectați la un singur canal de comunicație (*media-sharing*), atunci este nevoie de o modalitate de arbitraj pentru a stabili care dintre utilizatori poate transmite la un moment dat.

Metoda **CSMA/CD** (*Carrier Sense Multiple Access with Collision Detection*) permite accesul permanent la mediu al tuturor utilizatorilor, fără cereri prealabile pentru acordarea permisiunii de transmisie.

În principiu, aplicarea acestei metode presupune testarea sau "ascultarea" canalului de comunicații (*listening*) pentru detecția unei purtătoare pe linie (*carrier sense*). Dacă linia este liberă, atunci utilizatorul transmite date. Când două calculatoare transmit date simultan, apare o

coliziune și unul dintre pachete este distrus. Calculatorul-sursă este înștiințat de pierderea pachetului și este necesară retransmisia lui. Procesul de retransmisie introduce întârzieri care afectează negativ performanțele rețelei.

Acest inconvenient se rezolvă prin metoda **Token Passing** (în traducere, "jeton de trecere"). Fiecare utilizator cere permisiunea de transmisie și în momentul în care o are, transmite datele pe canal, în final primind confirmarea recepției corecte a lor la destinație.

Evident, metoda necesită capacitate suplimentară de procesare și timpi de transmisie a mesajelor de control (ENQ - *ENQuire* - cerere de transmisie; ACK - *ACKnowledge* - confirmare de primire; NAK - *Not Acknowledge* - pentru pachete neexpediate ș.a.) dar avantajul major este acela că nu apar coliziuni în rețea.

Uzual, în rețelele cu fir, de arie mică și viteză redusă, se utilizează procedeul CSMA/CD iar în cele de arie largă, cu rate mari de transmisie, se aplică metoda Token Passing.

O altă metodă de acces la mediu este cea la cerere, pe bază pe priorități (DPMA - *Demand Priority Media Access*), prin protocolul DPP (*Demand Priority Protocol*).

Pentru sistemele de transmisie 'fără fir' (*wireless*) se aplică metoda **CSMA/CA** (*CSMA with Collision Avoidance*) care încearcă evitarea apariției coliziunilor, prin transmiterea în prealabil de către stația emițătoare a unei cereri de acordare a permisiunii de transmisie din partea stației de destinație.

I.4.2 Topologia logică

Modul de expediere a mesajelor într-o rețea este descris prin topologia logică a acesteia.

Există **topologia logică de difuzare** (*broadcast logical topology*) în care mesajul este transmis tuturor terminalelor, fiind ignorat de cele cărora nu le este destinat.

A doua variantă de topologie logică este cea **secvențială** sau **"în inel"** (*ring logical topology*), care presupune transmiterea mesajului în rețea, treptat, de la un nod la altul. După citirea adresei-destinație, se decide la nivelul nodului dacă îi este adresat acestuia sau trebuie transmis următorului nod din rețea. Topologia logică secvențială are avantajul că reduce încărcarea rețelei dar timpul de transfer al mesajului crește comparativ cu topologia logică cu difuzare.

I.4.3 Topologia fizică

Modalitatea de interconectare a calculatoarelor și a celorlalte echipamente de comunicație definește topologia fizică a rețelei.

Frecvent, topologia rețelelor cu difuzare (PMP) este de tip "magistrală" (*bus*), "inel" (*ring*) sau "stea" (*star*) (Fig. I.9).

În rețeaua de tip "magistrală", la un anumit moment doar un singur calculator poate transmite date întrucât terminalele sunt conectate liniar la mediu, fie prin fir cu conectori, fie 'fără fir', folosind echipamente de transmisie-recepție (*transceiver*). Dezavantajul acestei rețele îl constituie posibilitatea de întrerupere totală a comunicației în cazul blocării canalului de transmisie.

Topologia de tip "inel" presupune trecerea mesajelor prin mai multe noduri ale rețelei. Dacă unul dintre terminale nu funcționează, rețeaua se blochează.

Rețeaua de tip "stea" este cea mai flexibilă și mai fiabilă ca topologie, prin **centralizarea** controlului traficului cu o structură de tip *master-slave*. În centrul rețelei este plasat un DCE care poate fi un concentrator (*hub*), un comutator (*switch*), un repetor (*repeater*) sau o unitate centrală de acces (CU - *Central Unit* sau MAU - *Multistation Access Unit*). Ieșirea din uz a unui calculator nu afectează comunicația dintre celelalte noduri ale rețelei. Conectarea unui nou calculator la rețea se poate face fără întreruperea funcționării acesteia, în limita numărului de porturi disponibile la nivelul nodului central.

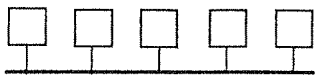
Existența echipamentului central de comunicație permite o mai bună monitorizare, securizare și administrare a rețelei.

Rețelele cu arie largă de răspândire (WAN) sunt de tip punct-la-punct (PP) având ca topologii fizice cele de tip "stea", "inel", "arbore" (*tree*), "plasă" (*mesh*) sau combinate (inel-stea, inel-inel etc) (Fig.I.9).

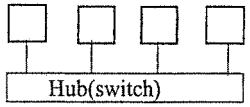
În rețelele WAN de tip "mesh", utilizate în cele mai multe cazuri, ruterele aleg căile optime de transmisie a pachetelor, pe baza tabelelor de rutare deduse prin analiza grafului care modelează matematic rețeaua. Protocoalele de rutare sunt aplicate în vederea alegerii rutei optime, în baza unui criteriu de optim care diferă de la un protocol la altul: timp minim de transmisie, cea mai scurtă cale, risc minim de coliziune a pachetelor etc.

Routerele și mediul fizic prin intermediul cărora se interconectează mai multe LAN-uri alcătuiesc o **subrețea de comunicație** (*subnetwork*) care funcționează conform celor trei nivele inferioare ale modelului OSI: fizic, legătură de date și rețea.Uneori protocoalele de rutare fac apel și la nivelul de transport pentru transmisia pachetelor numai spre anumite aplicații, în vederea reducerii încărcării rețelei sau pentru restricționarea accesului pe motive de securitate.

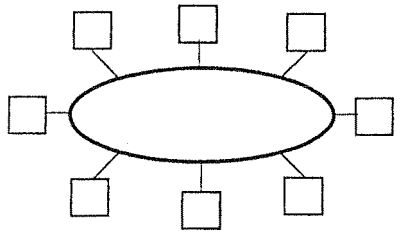
Avantajul topologiei *mesh* este acela că nu apar coliziuni între pachete, dar costurile necesare pentru achiziționarea materialelor și cele de instalare sunt relativ mari în comparație cu alte topologii fizice de rețea.



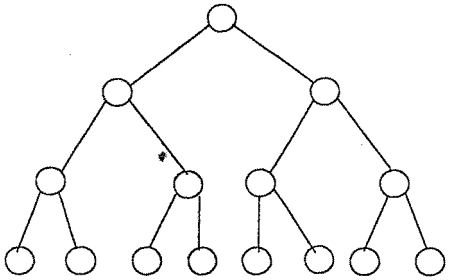
a. Topologie "magistrală"



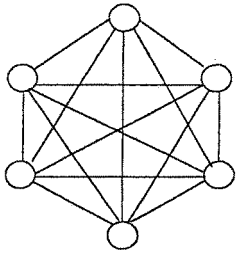
c. Topologie "stea"



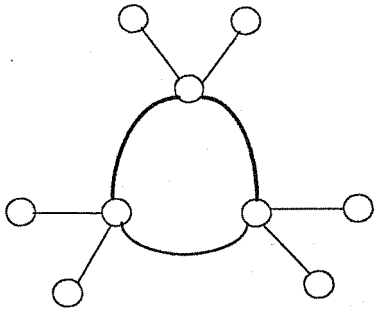
b. Topologie "inel"



d. Topologie "arbore"



e. Topologie "plasă"

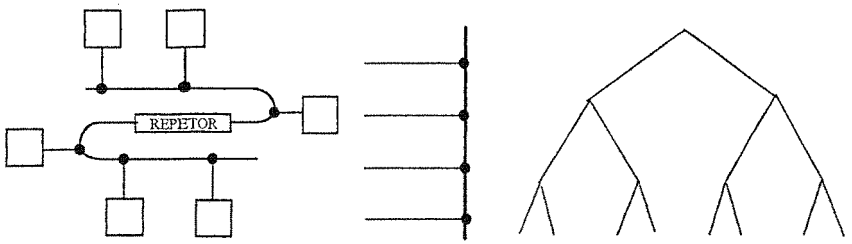


f. Topologie "inel-stea"

Fig.I.9 Topologii fizice de rețele

Pentru realizarea fizică a unei rețele cu transmisie pe cablu, **cablarea** (*wiring*) se poate face respectând diverse topologii (Fig.I.10):

1. **liniară** - un singur cablu este trecut prin toate punctele dorite iar calculatoarele se conectează la acesta în punctul cel mai apropiat; eventual între stațiile aflate la distanțe mai mari decât lungimea maximă admisă a segmentului de cablu, se pot intercala repetoare obținându-se astfel o rețea **segmentată;**



a. Liniară, segmentată b. "coloană vertebrală" c. 'arbore'

Fig. I.10 Topologii de cablu

2. de tip **"coloană vertebrală"** (*backbone*) - există cabluri orizontale și repetoare pe fiecare nivel, toate fiind conectate la cablul central care reprezintă "coloana vertebrală" a rețelei;

3. de tip **"arbore"** - este cea mai generală topologie și are avantajul că reduce riscul de coliziune în rețea. În plus, se pot conecta noi utilizatori în rețea fără modificarea structurii de cablare aferente celor existenți.

Numeroase probleme de transmisie sunt cauzate de defectele apărute în nodurile centrale ale unei rețele sau la nivelul mediului fizic de transmisie (cablu sau legătură prin undă radio). De aceea, este indicat ca în rețelele cu risc mare de întrerupere a întregului proces de transmisie, să existe rezerve de transmisie (*backup*), atât pentru calculatoarele de tip server (de exemplu, servere de nume), cât și pentru structurile de transmisie (cabluri sau linii de radioreleu). În cazul rețelelor cu topologie fizică de tip "inel", se poate folosi ca rezervă fie un al doilea inel de transmisie cu caracter redundant, fie o structură de cablare de tip "stea" cu un nod central denumit **centru de cablare** (*wiring center*), astfel încât defectarea unui nod al rețelei să nu afecteze toate comunicațiile din rețea. Sistemele de *backup* impun costuri suplimentare pentru realizarea rețelei dar asigură performanțe mai bune în funcționare.

II

PROTOCOALE DE COMUNICAȚII

II.1 SUITA DE PROTOCOALE TCP/IP

Suita TCP/IP gestionează toate transferurile de date din Internet, care se realizează fie ca **flux de octeți** (*byte stream*), fie prin unități de date independente denumite **datagrame** (*datagram*).

Protocoalele din această familie sunt ierarhizate pe cele patru nivele ale modelului TCP/IP (Fig. II.1). Protocoalele de pe nivelele superioare ale stivei beneficiază de serviciile furnizate de protocoalele de pe nivelele inferioare.

Numele acestei suite de protocoale este dat de protocolul de rețea (IP) și cel de transport (TCP). Totuși suita include mai multe protocoale deosebit de utile pentru furnizarea serviciilor Internet:

IP (*Internet Protocol*) - protocol de nivel rețea (Internet), prin intermediul căruia se transferă toate datele și care stabilește modul de adresare ierarhizat folosind adrese IP de 4 octeți, exprimați în format zecimal cu separare prin puncte (*dotted-decimal notation*), pentru localizarea sistematică a sursei și destinației, într-o anumită rețea sau subrețea de calculatoare (RFC 791). Încapsulează datele provenite de pe nivelul de transport sau de la celelalte protocoale de pe nivelul Internet (ICMP, IGMP), nivelul de rețea mai este denumit și **nivel IP**.

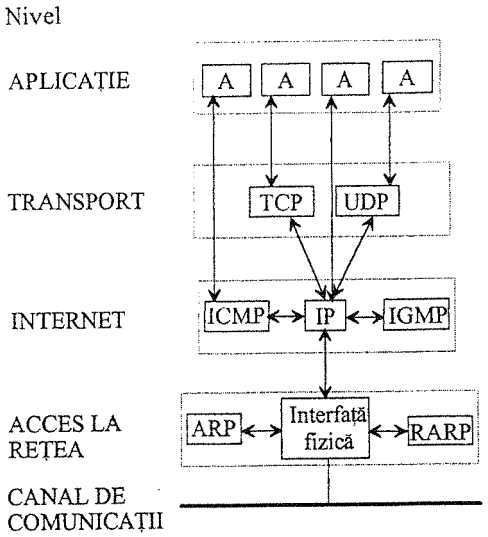


Fig.II.1 Comunicatii între protocoalele din stiva TCP/IP (A= aplicatie)

TCP (*Transport Control Protocol*) - protocol definit pe nivelul de transport, orientat pe conexiune, asemenea sistemelor telefonice. Permite controlul traficului, confirmarea sau infirmarea recepției corecte a mesajelor, retransmisia pachetelor și ordonarea corectă a fragmentelor unui mesaj.

UDP (*User Datagram Protocol*) - protocol de transport fără conexiune, asemănător sistemului poștal clasic, ceea ce îl face mai puțin sigur decât TCP dar mai puțin pretențios.

ICMP (*Internet Control Message Protocol*) - protocol de nivel rețea care transportă mesaje de control și de eroare, referitoare la capacitatea sistemului de a transmite pachetele de date la destinație fără erori (RFC 792). Protocolul ICMP comunică direct cu aplicațiile, fără a accesa TCP sau UDP.

IGMP (*Internet Group Management Protocol*) - gestionează transferul datelor spre destinații de grup, care includ mai mulți utilizatori, prin transmisii *multicast* (RFC 1112).

ARP (*Address Resolution Protocol*) - comunică la cerere, pe baza adresei IP a unui echipament, adresa fizică (MAC) de 6 octeți a acestuia (RFC 826). Tabelele ARP sunt stocate în memoria RAM a echipamentului (calculator, router etc). Se pot face echivalări sugestive între numele unei persoane și adresa MAC a echipamentului, respectiv între adresa poștală și adresa IP, care permit localizarea destinației unui mesaj.

RARP (*Reverse Address Resolution Protocol*) - furnizează la cerere adresa IP dată unui echipament cu adresa MAC, pe baza unor tabele (RFC 903).

ARP și RARP se utilizează numai în interiorul unui LAN. Aceste protocoale nu folosesc IP pentru încapsularea datelor.

Din figura II.1, se observă că un protocol de aplicație (A) poate comunica direct cu IP, dar în acest caz este nevoie să includă funcțiile de transport în propriul program de aplicație.

Ca protocoale de aplicații, care oferă direct servicii utilizatorului, se folosesc:

FTP (*File Transfer Protocol*) - protocol de transfer al fișierelor între calculatoare, mai precis un limbaj comun care permite comunicarea între orice sisteme de operare (DOS, UNIX etc) folosind programe FTP pentru client și server. FTP folosește TCP pentru transferul sigur al datelor (RFC 959).

TFTP (*Trivial File Transfer Protocol*) - mai puțin sofisticat decât FTP, acesta este folosit pentru transferul unor mesaje scurte prin UDP. Se impun tehnici de corecție a erorilor întrucât UDP nu generează confirmarea de recepție corectă a mesajelor (ACK) ca TCP (RFC 783, RFC 906).

TELNET (*Virtual Terminal Connection Protocol*) - protocol de terminal virtual care permite conectarea unui utilizator de la distanță la anumite calculatoare-gazdă, rulând programul *telnetd* al serverului. Se utilizează algoritmi de negociere cu terminalul respectiv, pentru a-i cunoaște caracteristicile. Acesta este văzut ca un terminal virtual cu care se poate comunica de la distanță, indiferent de caracteristicile lui fizice (RFC 854, RFC 856).

FINGER (*Finger User-information Protocol*) - protocol care permite obținerea de informații publice despre utilizatorii unei rețele.

SMTP (*Simple Mail Transfer Protocol*) - permite diferitelor calculatoare care folosesc TCP/IP să comunice prin poșta elelctronică (*e-mail/electronic-mail*). Acest protocol stabilește conexiunea punct-la-punct între clientul SMTP și serverul SMTP, asigură transferul mesajului prin TCP, înștiințează utilizatorul despre noul mesaj primit după care se desface legătura (RFC 821).

SNMP (*Simple Network Management Protocol*) - este folosit pentru supravegherea funcționării rețelelor bazate pe TCP/IP (controlul statistic al traficului, performanțelor, modului de configurare și securizare) utilizând bazele de informații de management (MIB), structurate pe baza unor reguli definite de SMI (*Structure of Management Information*) conform RFC 1155. Versiunea SNMP2 prevede posibilitatea aplicării unor strategii centralizate sau distribuite de management de rețea.

BOOTP (*BOOTstrap Protocol*) - este apelat de un utilizator pentru a-și afla adresa IP. Acest protocol folosește UDP pentru transportul mesajelor. Un calculator care folosește BOOTP, expediază un mesaj în rețea prin broadcast (pe o adresă IP cu toți biții '1'). Serverul de BOOTP

retransmite mesajul în toată rețeaua (*broadcast*) iar destinația își recunoaște adresa MAC și preia mesajul. Acest protocol nu poate lucra într-un sistem de alocare dinamică a adreselor IP, dar spre deosebire de RARP, acesta furnizează sursei atât adresa sa IP, cât și adresele IP ale serverului și ruterului (*default gateway*) folosit de LAN (RFC 951).

DHCP (*Dynamic Host Configuration Protocol*) - succesor al protocolului BOOTP, permite utilizarea unui număr limitat de adrese IP de către mai mulți utilizatori. Clientul solicită serverului DHCP o adresă IP. Acesta îi alocă o adresă dintr-un domeniu de adrese cunoscut, eventual îi furnizează și masca de rețea. Alocarea este rapidă și dinamică. Deși ruterele nu suportă transmisiile broadcast solicitate de ARP și RARP, ele permit aceste transmisii în cazul BOOTP și DHCP ceea ce facilitează comunicațiile dintre diverse LAN-uri.

HTTP (*HyperText Transfer Protocol*) - protocolul propriu al Web-ului, folosit de utilizatorii *web* și de serverele WWW pentru transferul unor fișiere de tip text, imagine, multimedia, în format special (*hypertext*), prin intermediul unui limbaj special HTML (*HyperText Markup Language*) folosind interfețe grafice pentru utilizatori (GUI - *Graphic Unit Interface*).

NTP (*Network Time Protocol*) - sincronizează ceasurile interne din două sau mai multe calculatoare, cu precizie de 1 - 50 ms față de timpul standard oficial (RFC 1305).

Există și alte protocoale pe nivelul de aplicații al suitei TCP/IP care oferă diverse servicii utilizatorilot din Internet. În general, lista serviciilor Internet disponibile pe un PC din rețea, conținând informații despre protocoalele utilizate și porturile de aplicații asociate se găsește într-un fișier special (SERVICES), conceput ca o bază de date.

Încapsularea datelor constă în adăugarea unor informații suplimentare la începutul (*header*), eventual și la sfârșitul (*trailer*) blocului de date, în funcție de protocol.

Datele circulă în stiva de protocoale de sus în jos, în cazul transmisiei, și de jos în sus, spre aplicații, la recepție. Datele sunt încapsulate la fiecare nivel de modulul software asociat protocolului după care sunt transmise nivelului inferior.

De exemplu, în cazul folosirii TCP ca protocol de transport pentru o aplicație rulată într-o rețea de calculatoare, încapsularea datelor se realizează în mai multe etape, la trecerea de pe un nivel pe altul, conform figurii II.2.

Pe nivelul de aplicații, datele utilizatorului sunt încapsulate cu un antet de aplicație într-un **mesaj de aplicație.**

TCP încapsulează mesajul-aplicație cu antetul TCP generând un **segment TCP.**

Dacă se utilizează UDP ca protocol de transport, atunci mesajul-aplicație precedat de antetul UDP alcătuiește o **datagramă UDP.**

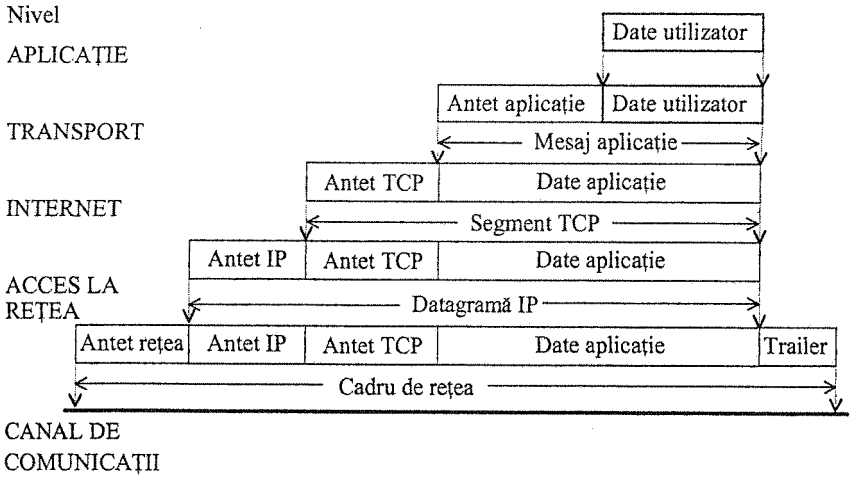


Fig.II.2 Încapsularea datelor în stiva TCP/IP folosind TCP

Unitatea generată de nivelul de transport este încapsulată cu un antet IP într-o **datagramă IP**, denumită uneori și pachet IP.

Driverul interfeței fizice de acces la rețea va încapsula datagrama IP într-un **cadru** care se transmite pe canalul fizic de comunicații.

Pe canalele sincrone, transmisia se poate face **serial,** ca flux de biți, sau **paralel,** sub formă de șir de octeți, în baza unui protocol de nivel fizic (HDLC - *High-level Data Link Control*, SLIP, PPP etc). Transmisiile în varianta "paralel" sunt admise numai pe distanțe relativ mici (de maximum 16 m).

În cazul comunicațiilor asincrone, se transmit unități de date individuale (5 - 8 biți), încapsulate cu un bit de **start** de nivel '0' logic (*low*) și biți de **stop** (1; 1.5 sau 2 biți), de nivel '1' logic (*high*). În intervalele de **pauză de transmisie**, se menține nivelul logic '1'. Este posibilă introducerea în cadrul datelor a unui bit de paritate (impară, pară etc) pentru detecția unui număr impar de erori de transmisie.

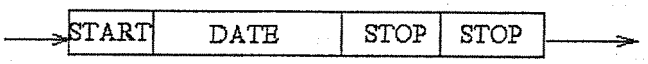


Fig.II.3 Cadru de transmisie asincronă

II.1.1 Protocolul INTERNET. Adresarea IP

Protocolul Internet (IP) constituie practic modulul de distribuție a datelor pentru rețelele de comunicații bazate pe TCP/IP. Toate protocoalele folosesc IP pentru transmisie, cu excepția celor de conversie a adreselor.

Adresarea ierarhică sistematică a utilizatorilor din Internet simplifică modul de administrare a acestuia. Adresele MAC nu sunt ierarhizate și localizarea destinației într-o rețea de arie largă este posibilă numai pe baza adreselor IP de 4 octeți, care specifică rețeaua, eventual subrețeaua în care se găsește un anumit calculator.

Protocolul Internet este considerat nesigur întrucât nu este orientat pe conexiunea dintre sursă și destinație dar permite identificarea corectă și în mod unic a oricărui echipament din rețea. Realizarea transferului datelor către aplicația-destinație devine sarcina nivelului de transport și a protocoalelor aferente acestuia.

Încapsularea datelor în formatul IP se face în **datagrame IP** sau **pachete IP** (RFC 1122), de minimum 576 octeți (B - Bytes) și cel mult 65535 octeți (64 kB). Ca terminologie, termenul de 'datagramă' reprezintă un serviciu de livrare, specificând formatul și conținutul unității de date, în timp ce se preferă utilizarea termenului de 'pachet' pentru unitățile de date neidentificate. Conform RFC 1122, 'pachetul' desemnează unitatea de date transferată între nivelul IP și cel de acces la rețea.

În funcție de arhitectura de rețea adoptată (Ethernet, Token-Bus, Token-Ring etc), datagramele IP trebuie fragmentate în mai multe cadre cu lungimea maximă admisă în rețeaua respectivă, așa-numita **unitate maximă de transfer** (MTU - *Maximum Transfer Unit*).

Formatul datagramei IP este prezentat în fig. II.4. Datele sunt precedate de un antet (*header*) de 20 sau 24 octeți, care include anumite câmpuri în care se specifică tipul de serviciu efectuat, gradul de securitate a transmisiei, detalii privind fragmentarea respectiv reasamblarea mesajelor de mari dimensiuni.

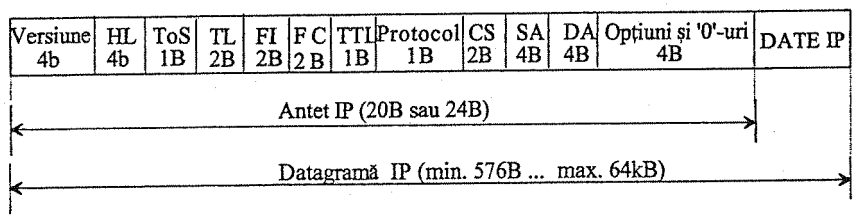


Fig. II.4 Formatul pachetului IP

Semnificațiile câmpurilor din antetul IP sunt următoarele:

Versiunea IP - este importantă pentru evitarea incompatibilității sistemelor.

HL - *Header Length* - precizează, în format binar, lungimea antetului în cuvinte de 32 de biți, adică 5 sau 6 cuvinte pentru includerea unor opțiuni. În general, acest câmp are valoarea 0101. Dacă se includ opțiuni atunci valoarea câmpului devine 0110.

ToS - *Type of Service* - poate preciza opt nivele de precedență sau diferite condiții: prioritate, întârziere minimă, debit maxim, siguranță maximă, cost minim (RFC 1349). Majoritatea ruterelor nu citesc acest câmp. De exemplu, o aplicație Telnet solicită întârzieri minime, pentru FTP se impune debit maxim, Usenet urmărește costuri minime iar SNMP este critic din punctul de vedere al siguranței transmisiei.

TL - *Total Length* - specifică pe 16 biți lungimea totală a pachetului exprimată în octeți (maximum 64 kB), inclusiv antetul IP.

FI - *Fragment Identification* - reprezintă un identificator (ID) al fragmentului de pachet util pentru reordonarea corectă a fragmentelor la destinație.

FC - *Fragment Control* - conține un indicator (*flag*) de 3 biți care precizează dacă datagrama este sau nu este fragmentată sau că acesta este ultimul fragment al ei. Ceilalți 13 biți indică poziția relativă a fragmentului în pachetul IP.

TTL - *Time-To-Live* - este un parametru care elimină riscul de propagare la infinit a unui pachet în rețea atunci când destinația nu este găsită. Poate fi inițializat cu valoarea maximă 255 dar se preferă valorile de 32 sau 16 pentru a evita supraîncărcarea rețelei. La fiecare ruter (*hop*), valoarea din câmp este decrementată cu 1. Când se ajunge la zero, pachetul este automat distrus.

Protocol - este un câmp care indică protocolul de nivel superior folosit pentru formatarea datelor din câmpul de date IP. Câteva valori tipice care pot fi înscrise în acest câmp sunt:

1 ICMP
2 IGMP
6 TCP
8 EGP (*Exterior Gateway Protocol*)
17 UDP
89 OSPF (*Open Shortest Path First*).

CS - *Checksum* - este un câmp de control a erorilor de transmisie la nivelul header-ului, care garantează corectitudinea antetului IP, nu și a datelor transferate.

SA - *Source Address* - adresa IP a sursei.

DA - *Destination Address* - adresa IP a destinației.

"Opțiuni" și '0'-uri - reprezintă un câmp opțional folosit pentru diagnosticare (de exemplu, folosind PING - *Packet InterNetwork Groper*), securizare sau setare a rutelor. Acest câmp este completat eventual cu zerouri astfel că lungimea header-ului crește cu 4 octeți atunci când se introduc diverse opțiuni.

ADRESAREA IP

O adresă IP este exprimată pe 4 octeți, în format zecimal cu puncte. Aceasta conține identificatorul de rețea (N - *network)*, eventual de subrețea (S - *Subnetwork*) care include echipamentul-gazdă și identificatorul plăcii de rețea a acestuia (H - *Host*). Identificatorul (ID - *IDentifier*) de rețea precede identificatorul plăcii de rețea. Adresa IP astfel formată este alocată în mod unic în Internet de InterNIC (*Internet Network Information Center*).

Schema de adresare IP este structurată pe cinci clase de adrese, diferențiate în funcție de lungimea câmpului alocat rețelei dar și prin prefixul binar utilizat (Tabel II.1) stabilit pe baza unui cod-prefix.

Adresele cu toți biții identici sunt rezervate ('1' - pentru *broadcast*; '0' - pentru rețea) și nu se alocă subrețelelor sau gazdelor.

Tabel II.1 Clasele de adrese IP

Clasa de adrese	Lungimea adresei rețelei (B)	Prefix binar fix	Domeniul de valori al primului octet	Lungimea ID-ului de rețea (b)	Lungimea ID-ului gazdei (b)	Numărul de calculatoare - gazdă adresabile	Număr de rețele adresabile
A	1	0	0 - 127	7	24	16 777 214	126
B	2	10	128 - 191	14	16	65 534	16 382
C	3	110	192 - 223	21	8	254	2 097 150
D	(multicast)	1110	224 - 239	-	-	-	-
E	(rezervată)	11110	240 - 247	-	-	-	-

În aceeași rețea se folosește un singur ID de rețea dar ID-uri de gazdă diferite. Se spune că adresele de clasă A, B sau C sunt de tip *unicast* deoarece identifică în mod unic gazda.

Simbolic adresele IP pot fi scrise astfel:

1. adrese de clasă A:

0NNN NNNN. HHHH HHHH. HHHH HHHH. HHHH HHHH

2. adrese de clasă B:

10NN NNNN. NNNN NNNN. HHHH HHHH. HHHH HHHH

3. adrese de clasă C:

110N NNNN. NNNN NNNN. NNNN NNNN. HHHH HHHH

De exemplu, rețeaua cu 4 calculatoare având adresele IP: 192.110.12.1; 192.110.12.2; 192.110.12.3; 192.110.12.4 are identificatorul de rețea 192.110.12.0.

Administrarea în mod unic a întregului spațiu de adrese din Internet este practic imposibilă, fiind vorba de circa 4 miliarde de adrese. De aceea s-a procedat la divizarea acestuia în rețele mai mici, cu număr redus de adrese care sunt administrate local de ISP (*Internet Service Provider*). Acest fapt a determinat reducerea numărului de adrese din Internet la circa 3,7 miliarde dar nu constituie un dezavantaj major deoarece alocarea adreselor se poate face dinamic, nu static (adresare fixă a gazdelor), numai pentru utilizatorii activi la un moment dat din rețea. Adresarea în interiorul LAN-ului poate fi făcută cu adrese locale alocate de administratorul de rețea și nu prin DNS, adrese care nu au legătură cu adresele IP reale date de DNS rețelei respective.

Observații

1. Adrese IP se alocă și unor interfețe fizice din echipamentele de comunicație (de exemplu, unui router i se pot aloca mai multe adrese IP, întrucât are mai multe interfețe de comunicație).

2. Pentru aplicații care necesită adresarea multicast se utilizează adrese de clasă D, în baza protocolului IGMP. Există adrese de grupuri prestabilite (*well-known*) de către IANA (*Internet Assigned Numbers Authority*) subordonată societății ISOC (*Internet SOCiety*) care coordonează funcționarea întregului Internet. Exemple de adrese multicast permanente (conform RFC 1112):

224.0.0.1 multicast către toate sistemele dintr-un LAN.

224.0.0.2 multicast către toate ruterele dintr-un LAN.

224.0.0.5 multicast către toate ruterele OSPF dintr-un LAN.

224.0.0.9 multicast pentru toate ruterele RIP-2 dintr-un LAN.

224.0.1.1 multicast pentru protocolul NTP (*Network Time Protocol*).

3. În multe cazuri chiar și 254 de adrese reprezintă un număr prea mare pentru o rețea de calculatoare locală. Se impune atunci partajarea unei clase de adrese (A, B, C) în mai multe subclase alocate **subrețelelor** (*subnetwork*) cu un anumit număr de utilizatori. Identificarea subrețelei se face în câmpul identificatorului gazdei, prin biții cei mai semnificativi. Numărul biților utilizați pentru identificatorul de subrețea, respectiv pentru ID-ul gazdelor, este restricționat la **minimum doi,** întrucât combinațiile de biți identici '1' sau '0' sunt rezervate.

Se observă faptul că pentru rețelele de clasă C se pot folosi minimum 2 și maximum 6 biți pentru ID-ul subrețelelor. În rețelele de clasă B, se pot defini subrețele folosind minimum 2, maximum 14 biți pentru ID-ul de subrețea.

De exemplu, pentru o subclasă de adrese de tip C cu subrețele de cel mult 6 utilizatori, se aplică formatul:

110N NNNN. NNNN NNNN. NNNN NNNN. SSSS SHHH

Se pot forma 30 subrețele fiecare cu maximum 6 utilizatori.

Interconectarea subrețelelor în LAN se poate realiza prin intermediul ruterelor interne. Interconectarea LAN-urilor în WAN se face prin rutere externe.

Rutarea pachetelor prin Internet presupune că la nivelul ruterelor externe se citește adresa rețelei (fără ID-ul gazdei), iar la nivelul ruterelor interne se extrage adresa subrețelei. Pentru aceasta se folosesc **măști de rețea** (*network mask*) pe care le aplicăm adresei IP a destinației pentru a selecta ID-ul rețelei, respectiv **măști de subrețea** (*subnetwork mask*) pentru determinarea adresei subrețelei. În acest scop, se efectuează operația 'ȘI' logic (AND), bit cu bit, între adresa IP a destinației și mască. Masca de rețea sau de subrețea se obține prin impunerea valorii '1' tuturor biților din câmpul rețelei, respectiv a subrețelei, și '0' pe toate pozițiile din câmpul gazdei.

Masca de rețea este definită pentru fiecare clasă de adrese IP:

1. masca de rețea în clasă A: 255.0.0.0
2. masca de rețea în clasă B: 255.255.0.0
3. masca de rețea în clasă C: 255.255.255.0.

Măștile de subrețea se particularizează în funcție de numărul de biți alocați acesteia.

Exemplul 1

Pentru citirea adresei rețelei în care se află calculatorul cu adresa 192.110.12.1 se aplică masca de rețea de clasă C: 255.255.255.0. În binar se obține:

Adresa IP a destinației:	1100 0000. 0110 1110. 0000 1100. 0000 0001
	AND
Masca de rețea:	1111 1111. 1111 1111. 1111 1111. 0000 0000
Rezultă ID-ul rețelei:	1100 0000. 0110 1110. 0000 1100. 0000 0000

Adresa acestei rețele este 192.110.12.0.

Exemplul 2

Pentru adresa IP 170.202.112.23, de clasă B, se aplică masca de rețea 255.255.0.0 rezultând adresa rețelei: 170.202.0.0.

Exemplul 3

Pentru rețeaua 192.110.12.0 cu masca de rețea este 255.255.255.0, se pot forma 30 de subrețele cu câte 6 utilizatori, folosind 5 biți din câmpul gazdei pentru subrețea.

Se folosesc deci 29 de biți pentru rețea și subrețea (*network bits*).

Masca de subrețea este: 11111111.11111111.11111111.11111000 sau 255.255.255.248.

Pentru aflarea numărului de identificare a gazdei în rețea sau subrețea, se aplică o combinație binară echivalentă măștii de rețea sau subrețea negate pe care o vom denumi simplu **masca negată** (*wild card*), având toți biții '0' în câmpul rețelei și subrețelei, respectiv '1' în câmpul gazdei.

Exemplul 4

Pentru rețeaua din exemplul 3, masca negată, în binar, este:

00000000.00000000.00000000.00000111

iar în format zecimal cu puncte rezultă 0.0.0.7.

Prima subrețea formată are adresa 192.110.12.8 și clasa de adrese pentru calculâtoarele-gazdă 192.110.12.9 ... 192.110.12.14. Adresa de broadcast a subrețelei este 192.110.12.15.

A doua subrețea are adresa 192.110.12.16, clasa de adrese a gazdelor 192.110.12.17 ... 192.110.12.22 și adresa de broadcast 192.110.12.23 ș.a.m.d. Similar se stabilesc adresele tuturor subrețelelor formate.

Observații

1. Pentru garantarea unicității adreselor IP utilizate în Internet, organizații naționale și internaționale alocă fiecărei rețele un număr unic de identificare ASN (*Autonomous System Number*), asemenea adresei fizice (MAC) a unui echipament.

2. Adresele IP ale interfețelor echipamentelor de comunicație (gateway, firewall, router) prin care se transportă pachetele între LAN și WAN, mai sunt denumite și **adrese de transport**. În general, este indicat ca unui echipament de comunicație să i se aloce o clasă de adrese separată. Rutarea pachetelor se va face pe baza tabelelor de rutare în care sunt stabilite rutele între adresele de transport.

3. Pentru lărgirea spațiului de adrese din Internet s-a propus folosirea **IPng** (*IP next generation*) sau IPv6 care, spre deosebire de IPv4, folosește adrese de 128 de biți, ordonate ierarhic; elimină broadcast-ul în favoarea multicast-ului; include în cadrul IP un header cu lungime fixă

conținând informații strict necesare rutării pachetelor, altele fiind incluse în subheadere; suportă modul automat de alocare a adreselor IP; permite autentificarea și criptarea datelor; prevede un sistem de priorități privind transmisia care să faciliteze transmisiile multimedia (voce, audio, video).

IPv6 poate procesa adresele date prin IPv4 dar DNS necesită un MIB (*Management Information Base*) suplimentar pentru stocarea numelor și adreselor de utilizator de 128 de biți.

APLICAȚII

1. Un calculator cu adresa 193.214.32.125 dorește să transmită în rețeaua locală un mesaj prin broadcast. Ce adresă IP a destinației utilizează? Care este adresa de broadcast pentru această rețea?

2. Administratorul de rețea transmite utilizatorilor din rețea un mesaj prin broadcast. Dacă adresa IP a sursei este 172.100.94.1care este adresa IP a destinației?

3. Sursa cu adresa IP 173.100.94.1 transmite un mesaj calculatorului cu adresa 192.100.10.120. Ce mască de rețea se aplică la nivelul ruterelor?

4. Unui LAN i se alocă ID-ul de rețea 193.125.117.0. Administratorul constată că îi sunt necesare subrețele cu maximum 30 utilizatori.

a. Câte subrețele poate forma?

b. Ce mască de subrețea se utilizează ?

c. Ce mască de rețea se aplică ?

d. Care sunt adresele subrețelelor respectiv clasele de adrese ale calculatoarelor-gazdă din fiecare subrețea?

e. Ce adrese de broadcast se utilizează în fiecare subrețea formată?

5. Pentru o adresă IP 203. 192.45.16 se folosește masca de subrețea 255.255.255.192. Determinați:

a. numărul de biți utilizați pentru ID-ul subrețelei;

b. numărul de subrețele existente în acest LAN;

c. adresele subrețelelor;

d. măștile de rețea, de subrețea și masca negată;

e. clasele de adrese și adresa de broadcast pentru a treia subrețea (în ordine crescătoare a adreselor de subrețea).

II.1.2 DNS - Sistemul numelor de domenii Internet

Deoarece este mai comod să se rețină nume sugestive pentru utilizatorii Internet decât adrese IP, a devenit necesară conversia acestor nume în adrese IP și invers folosind protocoale specifice de adresare precum și crearea unei baze de date care să stocheze aceste nume. Sistemul numelor de domenii Internet (DNS - *Domain Name System*) reprezintă o bază de date distribuită prin care se alocă adrese numerice celor de tip alfanumeric, folosind diagrame-arbore, MIB-uri și servere de nume, fiecare cu un anumit domeniu în care este autorizat să ruleze algoritmii de căutare (*authority zone*).

Asemenea claselor de adrese IP, și aceste nume de domenii sunt structurate ierarhic, astfel încât să fie posibilă gestionarea lor în bune condiții (pe criterii de timp, unicitate, accesibilitate în baza de date etc).

Numele nodurilor din Internet sunt compuse din mai multe **etichete** separate prin puncte (de exemplu, etc.tuiasi.ro), fiecare etichetă reprezentând numele unui **domeniu Internet** în care este inclus calculatorul respectiv. Un domeniu Internet este definit pe baza unor caracteristici de activitate sau de localizare, folosind o diagramă de tip 'arbore', cu un nod 'rădăcină' și mai multe nivele de ierarhizare (Fig. II.5).

Pe primul nivel, DNS este împărțit în trei domenii:

1. **ARPA** (*Advanced Research Projects Agency*) - domeniul responsabil de transformarea numelor de domenii Internet în adrese numerice (IP);

2. **grupul generic** al organizațiilor, cuprinzând șapte categorii de bază, fiecare asociată unei etichete compusă din trei caractere (Tabel II.2).

3. **grupul geografic** al țărilor, specificate prin etichete cu două caractere stabilite de ISO (ISO 3166). De exemplu, ro - România, us - Statele Unite ale Americii, uk - Marea Britanie.

Tabel II.2 Grupul generic din Internet

Etichetă	Descrierea domeniului
com	organizație comercială
edu	organizație educațională
gov	organizație guvernamentală (rezervat S.U.A.)
int	organizație internațională (rezervat S.U.A.)
mil	organizație militară
net	rețea propriu-zisă neinclusă în alte categorii
org	alte organizații (cu specific noncomerial, nonguvernamental etc)

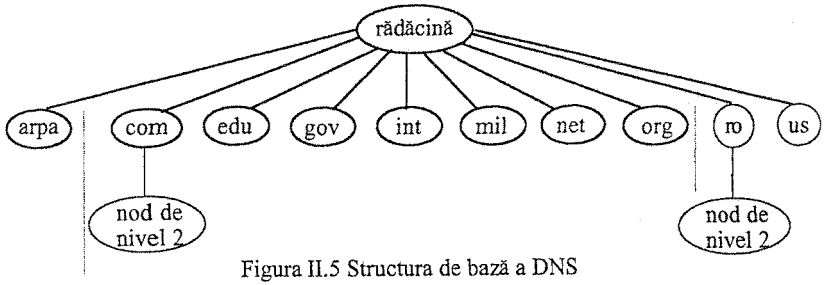


Figura II.5 Structura de bază a DNS

Fiecărui nod de pe primul nivel al diagramei îi corespund mai multe noduri de nivel 2, care la rândul lor au legături cu noduri de nivel 3 ș.a.m.d., rezultând o diagramă mult ramificată, dar structurată ierarhic pe principiul prefixului. Astfel se realizează identificarea în mod unic a fiecărui domeniu și subdomeniu Internet.

InterNIC gestionează numai domeniile de pe primul nivel, subdomeniile fiind în responsabilitatea unor organizații regionale, respectiv a administratorilor fiecărei rețele locale.

Deoarece numărul subdomeniilor Internet este foarte mare, nu este indicată crearea unei baze de date unice pentru memorarea tuturor numelor din Internet, ci s-a preferat realizarea unei **baze de date distribuite** care memorează datele pe mai multe calculatoare dedicate programelor server de nume, numite simplu **servere de nume** sau **servere DNS**. Fiecare server gestionează calculatoarele dintr-un subdomeniu sau **zonă**, adică o anumită clasă de adrese IP.

Programul-client pentru translarea numelor de domenii Internet apelează o funcție de translare a adreselor (de exemplu, *gethostbyaddr, gethostbyname*), care deschide un canal de comunicație cu programul-server DNS, transmite cererea și după ce primește de la server informația despre adresa respectivă, închide canalul și transmite informația programului-client.

În funcție de modul în care serverul DNS răspunde cererii unui program-client DNS de translare a numelor (*name resolver*) și furnizare a adresei IP asociate unui domeniu Internet, neinclus în baza de date proprie, aceste servere sunt de două tipuri:

1. **iterative** - răspunde negativ clientului, indicându-i acestuia să continue căutarea pe alt server de nume.

2. **concurențiale (recursive)** - rezolvă cererea prin contactarea altor servere DNS.

Pentru evitarea blocării unei rețele prin defectarea serverului DNS, este recomandată utilizarea a cel puțin un server de nume secundar sau de rezervă (*backup*), care deține o copie a bazei de date de pe serverul primar, periodic reactualizată. Prin utilizarea bazei de date distribuite

pentru DNS și a serverelor de nume secundare crește siguranța funcționării sistemului numelor de domenii Internet.

Un server de nume primar nu dispune de adresele tuturor celorlalte servere similare din DNS, ci cunoaște numai adresa serverului de nume 'rădăcină', de pe primul nivel al diagramei DNS, memorată în fișierul său de configurare. Fiecare server de nume 'rădăcină' are memorate numele și adresele tuturor serverelor de nume de pe nivelul 2. În general, fiecare server deține o bază de date în care sunt incluse numele și adresele altor servere de pe nivelele învecinate în vederea redirecționării cererilor pe care nu le poate soluționa.

Lista completă a serverelor de nume 'rădăcină' se găsește pe Internet, în fișierul netinfo/root_server.txt .

II.1.3 Protocoale de adresare (ARP, RARP, BOOTP, DHCP)

Echipamentele conectate în rețea (plăci de rețea, modemuri etc) sunt descrise prin așa-numita **adresă fizică**, dată de producător. Aceasta este exprimată pe șase octeți, în format hexazecimal și este unică în lume, fapt asigurat de modul de alocare a adresei: primii trei octeți identifică firma producătoare (OUI - *Organizational Unique Identifier*) iar ultimii trei, cei mai puțin semnificativi, sunt alocați de către producător, echipamentului.

Adresa fizică se mai numește și **adresă MAC** întrucât este folosită pentru acces la mediul fizic de transmisie, pe subnivelul MAC al nivelului legăturii de date din modelul OSI.

Rutarea pachetelor în WAN nu se face pe baza adreselor fizice, ci pe a celor de rețea, conform ierarhiei stabilite prin sistemul numelor de domenii. Prin urmare, este necesară conversia adreselor de rețea în cele fizice și invers. Pe baza adreselor fizice și a celor de rețea se realizează încapsularea datelor pe nivelele OSI 2 și 3.

Un router are incorporate mai multe plăci de rețea, fiecare cu o adresă de rețea proprie. Adresa IP alocată interfeței ruterului prin care o rețea locală se conectează la WAN, trebuie să fie din clasa de adrese a LAN-ului. Această adresă este considerată ca adresă implicită a porții de acces în WAN (*default gateway*).

Adresa de rețea poate fi alocată unei interfețe în mod static sau în mod dinamic. **Static**, se stabilește de către administratorul de rețea și este setată în fișierul de configurare al echipamentului (stație terminală, router etc). Există riscul să se aloce aceeași adresă mai multor utilizatori, ceea ce creează erori de trafic sau face imposibilă conectarea stațiilor în rețea. Administratorii de rețea trebuie să aibă o evidență clară a adreselor alocate pentru a evita duplicarea lor. De aceea, în rețelele de amri dimensiuni, se preferă **metoda dinamică** de alocare a adreselor de rețea, care face

ca un anumit spațiu de adrese să fie folosit de mai mulți utilizatori. În acest caz, un utilizator nu va avea aceeași adresă la fiecare conectare. Metoda are dezavantajul că filtrarea traficului pe baza adreselor de rețea devine ineficientă.

În suita de protocoale TCP/IP, se utilizează mai multe protocoale de adresare: ARP, RARP, BOOTP, DHCP.

Protocolul ARP (*Address Resolution Protocol*) realizează conversia adreselor IP în adrese MAC, pe baza unor tabele ARP (RFC 826).

Unele sisteme de operare (Windows 9x, Windows NT) folosesc ARP pentru a se asigura că nu există adrese IP duplicate. Cererea ARP (exprimând "Care este adresa ta MAC?") se transmite în rețeaua locală în modul broadcast. Dacă adresa IP respectivă este alocată altui nod din rețea, atunci sistemul de operare nu inițializează suita TCP/IP și generează un mesaj de eroare.

Transmisiile broadcast încarcă rețeaua. De aceea, se preferă păstrarea în memoria *cache* (de tip RAM) a tabelelor ARP, în care se stabilesc corespondențele dintre adresele fizice și adresele IP uzuale (*bindings*). În cazul alocării dinamice a adreselor, anumite informații din aceste tabele pot fi rejectate dacă nu sunt accesate în mod curent.

Cererea ARP (*ARP Request*) este transmisă în rețea numai dacă adresa solicitată nu există în tabelul ARP. Pachetul cu cererea ARP conține adresa MAC de broadcast, adresa MAC a sursei, adresele IP ale sursei și destinației, precum și un cod de cerere ARP (Fig.II.6). Stația de destinație din rețeaua locală răspunde printr-un alt pachet (*ARP Reply*) adresat stației care a inițiat cererea, pachet care include adresa sa MAC.

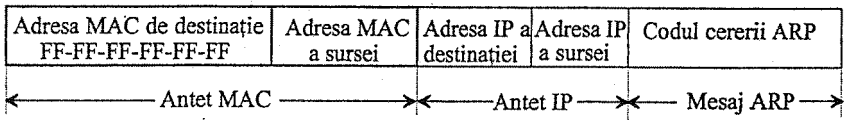


Fig.II.6 Formatul pachetului conținând cererea ARP

Când recepționează pachetul de răspuns, sursa își completează tabelul ARP cu noile adrese (MAC și IP).

Dacă sursa nu primește nici un răspuns, atunci cererea este retransmisă. Dacă nici la retransmisie nu se răspunde, sursa recepționează un mesaj de eroare generat de protocolul ICMP.

În cazul în care destinația nu se află în rețeaua locală, ruterul de legătură cu WAN-ul răspunde cu propria sa adresă, prin tehnica numită **Proxy ARP** (RFC 1027), dacă prin configurarea conexiunii gazdei cu rețeaua nu este dezactivată opțiunea *proxy*.

Protocolul RARP (*Reverse Address Resolution Protocol*) face conversia inversă, a adreselor fizice în adrese de rețea.

Dacă o stație de lucru nu-și cunoaște adresa IP, atunci trimite serverului RARP un pachet cu o cerere RARP (cu semnificația "Care este adresa mea IP?"), în modul broadcast (pentru Ethernet, se folosește adresa IP de destinație cu toți biții din câmpul gazdei egali cu '1').

Pachetul RARP include adresele MAC ale sursei și destinației, adresa IP de broadcast, un câmp de adresă IP necompletat pentru adresa IP proprie și codul cererii RARP, conținut în memoria sa ROM (Fig.II.7). Serverul RARP răspunde cererii cu un pachet conținând adresa IP solicitată.

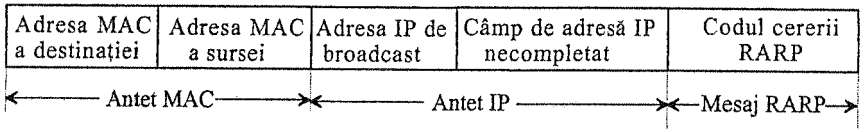


Fig.II.7 Formatul pachetului conținând cererea RARP

Observație

Routerele nu retransmit în afara LAN cererile ARP/RARP în mod broadcast, evitând propagarea infinită a lor în WAN.

Protocolul BOOTP (*BOOTstrap Protocol*) este apelat de un utilizator pentru a-și afla adresa IP (RFC 951). Acest protocol folosește UDP pentru transportul mesajelor și IP pentru încapsulare, fiind un protocol de nivel aplicație din suita TCP/IP.

BOOTP a fost inițial proiectat pentru stațiile de lucru fără disc, pe care nu erau memorate informațiile de configurare IP. Pe serverul BOOTP există o bază de date în care se stochează adresele MAC ale stațiilor din LAN și adresele IP asociate fiecăreia, în mod static. Un calculator care folosește BOOTP, expediază cererea de aflare a adresei IP proprii (*BOOTP Request*) în rețea, prin broadcast (pe o adresă IP cu toți biții '1'). Serverul BOOTP transmite automat răspunsul (*BOOTP Reply*) în toată rețeaua prin broadcast, iar destinația își recunoaște adresa MAC și preia mesajul.

Acest protocol nu poate lucra într-un sistem de alocare dinamică a adreselor IP, dar spre deosebire de RARP, el furnizează sursei atât adresa sa IP, cât și adresele IP ale serverului și ruterului (*default gateway*) folosit de LAN.

Protocolul BOOTP este rutabil și cererile clienților BOOTP sunt retransmise de router în afara LAN, prin **agentul de retransmisie BOOTP** (*BOOTP Relay Agent*) definit în RFC 1542. Acesta permite retransmisia prin router a răspunsurilor BOOTP către clienții conectați direct la router, dar și pentru clienții din alte rețele, întrucât mesajul BOOTP este tratat sub formă de pachete IP și retransmis unicast, multicast sau broadcast (*forwarding*) între rețelele locale din WAN, cu limitarea numărului maxim de noduri (*hops*) prin care trece pentru a nu încărca inutil rețeaua.

Protocolul DHCP (*Dynamic Host Configuration Protocol*) este succesorul protocolului BOOTP. DHCP permite utilizarea unui număr limitat de adrese IP de către mai mulți utilizatori prin metoda alocării dinamice (RFC 1541).

Clientul transmite cererea DHCP prin broadcast, cu adresa MAC proprie, pentru a i se aloca o adresă IP. Serverul DHCP îi răspunde clientului, identificat pe baza adresei MAC, oferindu-i o adresă IP și o mască de rețea, cu o perioadă de valabilitate prestabilită. Clientul transmite serverului un mesaj de acceptare după care acesta îi confirmă primirea acceptului (ACK - *Acknoledge*) și îi furnizează informații suplimentare despre serverul DNS și gateway-urile disponibile.

Alocarea este rapidă și dinamică, protocolul fiinddeosebit de util pentru terminale mobile și pentru serviciul de roaming în WAN.

Observații

1. Întrucât DHCP alocă dinamic adresele IP și identificarea stațiilor se face pe baza numelor, apar probleme de actualizare a bazelor de date de pe serverele DNS. De aceea, se preferă utilizarea DHCP cu servere WINS (*Windows Internet Name Service*)
2. Deși ruterele nu suportă retransmisiile broadcast solicitate de ARP și RARP, ele permit aceste retransmisii în cazul BOOTP și DHCP, ceea ce facilitează comunicațiile dintre diverse LAN-uri.
3. Suplimentar față de metoda alocării dinamice, DHCP suportă și modul automat, și modul manual de alocare a adreselor într-o rețea TCP/IP. Modul automat presupune alocarea de adrese IP permanente nodurilor din LAN. În modul automat, DHCP este utilizat doar pentru intermedierea procesului de negociere a adresei, dintre administratorul de rețea și stația-gazdă.

În multe rețele, doar un număr mic de utilizatori dintr-un subdomeniu privat (*stub domain*) comunică în afara rețelei, celelalte comunicații realizându-se local. În general, acestor domenii li se alocă doar câteva adrese IP reale (în particular, o singură adresă). Se pot utiliza local, în mai multe subdomenii, aceleași adrese IP private, fiind necesară translarea lor în adrese IP publice doar pentru comunicațiile cu exteriorul. Pentru aceasta, echipamentele prin care un subdomeniu este interconectat în LAN sau WAN sunt configurate să aplice **procedeul de translare a adreselor** (NAT - *Network Address Translation*), definit în RFC 1631, pe baza unor tabele de translare. În fiecare punct de ieșire din subdomeniu, adresa IP a sursei din fiecare pachet care urmează a fi transmis în Internet este translată, în mod static sau dinamic, într-o adresă IP globală, rezervată pentru NAT (RFC 1597).

Procedeul **NAT extins** (ENAT - *Enhanced Network Address Translation*) este utilizat pe scară largă în rețelele TCP/IP private (*stub domain*), care solicită o singură adresă IP globală din partea furnizorului de servicii Internet (ISP - *Internet Service Provider*). Ruterele de acces în WAN translează adresa IP a sursei în adresa IP globală și numărul portului de protocol în cel prestabilit. Procedeul ENAT asigură o bună securitate la nivelul firewall-ului, o mare flexibilitate în alegerea ISP, dar are ca dezavantaj reducerea vitezei de transfer prin procesul de modificare a antetelor și a sumelor de control din pachetele transmise. Există mai multe moduri de aplicare a procedeului ENAT: static, dinamic sau bazat pe tipul interfeței de acces în Internet.

Translarea statică a adreselor IP permite accesarea rețelei de oriunde din Internet, eventual numai pe un anumit port de protocol. Metodele dinamice de translare asigură o mai bună securitate a rețelei, prin limitarea accesului din afara acesteia.

II.1.4 Protocoale de transport (TCP,UDP)

În suita de protocoale TCP/IP, pe nivelul de transport se pot folosi două protocoale, **TCP** (*Transport Control Protocol*) și **UDP** (*User Datagram Protocol*), care oferă servicii de transport protocoalelor de aplicație.

Protocolul TCP este orientat pe conexiunea punct-la-punct dintre sursă și destinație, realizând transferul sigur al informațiilor, fără erori. TCP folosește mesaje de confirmare a recepției corecte a fiecărui pachet și cere retransmisia celor eronate.

Mesajul de pe nivelul aplicație este fragmentat în mai multe secvențe, pentru a nu depăși lungimea maximă admisă a unității de date transmise pe nivelul fizic (MTU - *Maximum Transmission Unit*). Datele sunt este încapsulate cu antetul TCP (Fig. II.8) și generate ca **segment TCP.** Acesta devine câmpul de date în datagrama IP. La recepție, TCP este responsabil de refacerea mesajului prin asamblarea corectă a tuturor secvențelor sale.

În antetul TCP sunt specificate, pe 16 biți, **numerele porturilor logice** asociate aplicațiilor sursă și destinație, între care se stabilește comunicația virtuală. Fiecare capăt al conexiunii TCP se numește *socket.*

Fiecare secvență dintr-un mesaj de aplicație este indexată printr-un **număr de secvență** (*SN - Sequence Number*) care permite asamblarea lor în ordine corectă, la recepție.

Numărul de confirmare (ACK n) specifică recepția corectă a secvențelor transmise și precizează numărul următoarei secvențe așteptate.

Lungimea antetului (HLEN - *Header Length*) este exprimată în cuvinte de 32 de biți și poate avea valorile 5 sau 6, în funcție de existența unor opțiuni în antet.

biți 0 4 10 15 16 31

Numărul portului sursă			Numărul portului destinație
Număr de secvență			
Număr de confirmare			
Lungimea antetului	Câmp rezervat	Biți de control	Lungimea ferestrei TCP
Sumă de control			Pointer al datelor urgente
Opțiuni			Câmp nul

Fig.II.8 Formatul antetului TCP

Biții de control (*flag*) specifică anumite funcții de control:

URG (*Urgent*) - indică receptorului existența unor date urgente;

ACK (*Acknowledge*) - arată receptorului existența unui număr corect de confirmare;

PSH (*Push*) - forțează receptorul să transmită imediat alte date;

RST (*Reset*) - cere receptorului să reinițializeze conexiunea;

SYN (*Synchronize*) - solicită receptorului să sincronizeze secvențele din mesaj;

FIN (*Final*) - specifică sfârșitul transmisiei.

Stabilirea unei conexiuni TCP se face în trei pași (*Three-Way Handshake Open Connection*), în care se folosesc acești biți pentru controlul fluxului și inițierea numerelor de secvență (SN) în ambele sensuri (Fig. II.9).

Segmentele TCP se pot transmite mai multe într-o sesiune, înainte de primirea unei confirmări de recepție corectă, într-un grup denumit **fereastră** (*window*).

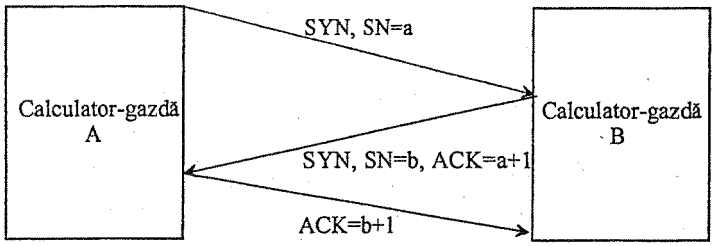


Fig. II.9 Algoritmul în trei pași de deschidere a conexiunii TCP

În antetul TCP se specifică lungimea ferestrei ca număr de octeți. Utilizarea ferestrei glisante (*sliding window*) permite controlul fluxului și creșterea vitezei de transmisie, respectiv a lățimii de bandă a rețelei.

Suma de control se calculează pentru tot segmentul TCP, fiind aplicată antetului împreună cu câmpul datelor.

Dacă există date transmise în **modul urgent** (de exemplu, caracterele *escape* sau *întrerupere* într-o aplicație Telnet), atunci în antet se specifică poziția ultimului octet al secvenței de date urgente.

În câmpul facultativ **opțiuni**, se poate specifica lungimea maximă a segmentului TCP (valoarea sa implicită este de 536 octeți).

Comunicația prin TCP se realizează în mod duplex, astfel că închiderea conexiunii impune oprirea fluxurilor de date din ambele sensuri, în două etape (*Two-Way Close Connection*), prin activarea flagului FIN spre ambele părți.

TCP folosește porturi de aplicație sau de protocol pentru a realiza comunicații simultane cu mai multe programe. Numerotarea porturilor de protocol se face global, în mod unic, pe întregul Internet și este descrisă în RFC 1700 (Tabel II.3). Aceste numere de protocol sunt utilizate atât de TCP, cât și de UDP.

Aplicațiilor publice li se rezervă numere de port mai mici decât 255.

Numerele mai mari ca 256 și mai mici decât 1023 sunt alocate aplicațiilor dezvoltate de anumite companii.

Valorile mai mari ca 1024 sunt alocate în mod dinamic pentru portul sursă.

Anumite numere de porturi de aplicații sunt utilizate numai de TCP.

Protocolul UDP (*User Datagram Protocol*) este considerat nesigur deoarece nu este orientat pe conexiune, nu utilizează mesaje de confirmare a recepției corecte, nu face retransmisia pachetelor eronate, nu permite controlul fluxului informațional și nu asamblează secvențele în cazul mesajelor fragmentate.

Avantajul acestui protocol este dat de viteza mare de procesare a datelor comparativ cu TCP.

Mesajul generat de nivelul aplicație formează împreună cu antetul UDP de 8 octeți o **datagramă UDP** (Fig. II.10).

Portul-sursă	Portul-destinație	Lungime	Sumă de control

Fig. II.10 Formatul antetului UDP

În antet se specifică, pe câte doi octeți, numerele porturilor de aplicație corespondente, lungimea datagramei și suma de control a antetului, pentru asigurarea corectitudinii adreselor.

Tabel II.3 Numerotarea porturilor logice de protocol

Protocol de aplicație din suita TCP/IP	Numărul portului alocat
Echo Protocol	7
Active Users	11
Daytime Protocol	13
FTP	21
SSH	22
Telnet	23
SMTP	25
TIME	37
RLP	39
NAME SERVER	42
NICNAME	43
DNS	53
BOOTP server	67
BOOTP client	68
TFTP	69
GOPHER	70
FINGER	79
HTTP*	80
POP2	109
POP3	110
Authentication Service*	113
UUCP Path Service*	117
NTP	123
NetBIOS Service	139
SNMP	161

* valabil numai pentru TCP

Observație

IP este un protocol fără conexiune, asemenea UDP. Ambele protocoale de transport din suita TCP/IP folosesc protocolul Internet pe nivelul rețea.

II.1.5 Protocolul Telnet

Protocolul TELNET *(Terminal Connection)* permite accesarea de la distanță a anumitor sisteme sau programe, prin operația de specificare a unui nume de utilizator și a unei parole (*remote login*).

Acest protocol rezolvă incompatibilitățile dintre două sisteme implicate într-o conversație în rețea, prin folosirea conceptului de **terminal virtual de rețea** (NVT - *Network Virtual Terminal*), prin care se specifică anumite caracteristici de bază ale unui terminal simplu (*dumb*). De exemplu, VT100 este un NVT. Programele care comunică în rețea prin Telnet convertesc datele în formatul impus de NVT.

Specificațiile Telnet (RFC 854) impun pentru NVT codul ASCII de codare a datelor în rețea, cu șapte biți pe caracter, prin care se pot reprezenta în binar 95 de caractere printabile și 33 de coduri de control.

NVT ASCII utilizează numai o parte din secvențele de control definite de ASCII (Tabel II.4)

Tabel II.4 Secvențe de control NVT ASCII

Secvență de control	Cod hexazecimal	Semnificație
NUL	0x00	*no operation*
BEL	0x07	*bell*
BS	0x08	*backspace*
HT	0x09	*horizontal tab*
LF	0x0A	*line feed*
VT	0x0B	*vertical tab*
FF	0x0C	*form feed*
CR	0x0D	*carriage-return*

De exemplu, combinația CR-LF reprezintă terminația standard pentru o linie conform formatului NVT ASCII.

Suplimentar, se introduce bitul al 8-lea, cel mai semnificativ din octet, pentru definirea și a altor secvențe de control.

Formatul NVT ASCII, definit de specificațiile Telnet, este utilizat și de alte protocoale de aplicație din suita TCP/IP.

Telnet este inclus în gama de servicii Internet oferite de rețeaua TCP/IP, specificate în baza de date cu servicii de rețea, în care sunt stocate numele protocolului, numărul portului asociat și, eventual, numele echivalent (*nickname*). Pe un PC, această bază de date se găsește în fișierul services, în format ASCII.

Utilizarea Telnet permite accesul de la distanță la stația de destinație.

Comanda de conectare pe un terminal din rețea folosind Telnet include fie adresa IP (*ipadd*) a terminalului pe care se dorește să se conecteze clientul Telnet, fie numele calculatorului, simplu dacă este în aceeași rețea sau incluzând numele domeniului Internet din care face parte dacă aparține altui segment de rețea. De asemenea, se poate specifica un nume echivalent (nickname) cu condiția ca acesta să fie inclus în baza de date de utilizatori de pe serverul de nume.

Este mai simplu de accesat o stație prin Telnet folosind numele prescurtat al terminalului sub forma unei combinații sugestive și accesibile de caractere (*nickname*), care poate fi definită printr-o comandă de asociere a acestuia cu adresa IP a stației respective (set).

Lista numelor calculatoarelor-gazdă incluse în baza de date poate fi afișată pe ecran cu comanda de vizualizare (show).

TTY (*TeleTYpe*) reprezintă denumirea echivalentă a terminalului virtual, fiind împrumutată din sistemul de operare UNIX.

Prin comanda de conectare sau comanda telnet, se creează temporar un TTY pentru serviciul respectiv și un alt TTY pentru portul accesat.

Conexiunea se realizează inițial cu parametrii impliciți pentru terminalul accesat, cu posibilitatea negocierii altor parametri pentru facilitarea comunicării.

Stabilirea tipului de terminal (de exemplu: dumb, vt100) accesat într-o sesiune Telnet se face prin comanda de definire a acestuia (set).

Se pot deschide mai multe sesiuni Telnet simultan.

Alte comenzi, valabile și pentru alte servicii de comunicații din Internet, sunt definite pentru crearea serviciului (create), eliminarea serviciului (destroy), conectare (connect), deconectare (disconnect), reconectare (reconnect), vizualizare a sesiunilor, serviciilor sau parametrilor de terminal virtual (show).

Observații

1. Protocolul Telnet poate fi utilizat pentru încărcarea sau accesarea de la distanță a fișierelor de configurare a unor echipamente de comunicație din rețea (*bridge, router, firewall*) de către personalul autorizat.

2. Sintaxa comenzilor protocolului depinde de firma producătoare a echipamentelor.

II.1.6 Protocolul Finger

Finger este un protocol simplu de tip serviciu Internet, bazat pe modelul client-server, care permite unui client Finger să obțină de la un server Finger informații cu caracter public despre un anumit utilizator sau despre toți cei activi în rețea, la un moment dat.

Interogarea serverului Finger se face pe portul de protocol 79 și se exprimă în formatul NVT ASCII definit de Telnet, având ca simbol de sfârșit de linie combinația de caractere CR-LF (*Carriage Return - Line Feeder*).

Serviciul Finger este orientat pe conexiunea dintre două socket-uri (prin socket, se înțelege un pointer la o structură de date memorată într-un buffer). După stabilirea conexiunii folosind TCP, se transmite cererea Finger.

Dacă apelul e realizat printr-o linie vidă (numai CR-LF), atunci serverul răspunde cu lista completă a tuturor utilizatorilor conectați la server în acel moment. Comanda folosită în acest caz este:

finger

Dacă lista completă a utilizatorilor are o dimensiune care depășește lungimea maximă a unității de transmisie din rețea (MTU), atunci TCP transmite datele în mai multe segmente de mesaj.

Comanda de interogare Finger poate să includă numele real al unui utilizator conectat la server:

finger {nume}

sau ID-ul utilizatorului și numele calculatorului-gazdă, cu sintaxa:

finger {nume_utilizator}@{nume_calculator_gazda}

Răspunsul constă în informațiile disponibile despre acesta: numele de utilizator, numele real al persoanei, contul curent al acesteia (*home directory*), ultima dată la care s-a conectat la rețea, numele stației la care s-a făcut conexiunea, informații privind folosirea serviciului de poștă electronică de către utilizator etc.

Dacă serverul Finger recepționează orice în afara unei linii vide, atunci acesta presupune că textul identifică un anumit utilizator și returnează toate informațiile publice despre utilizatorii cu numele sau ID-ul asemănător textului.

Serverul Finger transmite mesajul de răspuns stației sau sesiunii Telnet de la care s-a inițiat cererea. Clientul recepționează datele fie sub forma unui șir de octeți (*byte stream*), fie prin datagrame, și le memorează într-un buffer local. În cazul în care volumul datelor depășește

capacitatea de memorare a acestuia, atunci datele se pierd și se returnează un mesaj de eroare. Clientul recepționează un mesaj de eroare, prin intermediul ICMP, deși conexiunea a funcționat corect și transmisia este considerată reușită.

Serverul Finger închide automat conexiunea după ce a transmis toate datele solicitate.

Pe durata unei conexiuni active, este necesară aplicarea unor măsuri de securitate pentru a evita accesul nedorit al unui utilizator neautorizat la resursele unui calculator-gazdă implicat în acea conexiune. Un server Finger poate fi configurat astfel încât o cerere Finger adresată lui de la distanță, să inițieze pe server un fișier capabil să ruleze comenzi de sistem (*scripting*).

II.1.7 Protocoale de poștă electronică (SMTP, POP)

Poșta electronică (*e-mail / electronic mail*) este unul dintre cele mai utilizate servicii de comunicații din Internet.

Într-o rețea de calculatoare, sistemul de poștă electronică are următoarele componente (Fig.II.11):

1. memorie de stocare a mesajelor ce urmează a fi transmise ("coadă de ieșire");
2. procesul client de mail;
3. procesul server de mail;
4. cutiile poștale (*mailbox*) ale utilizatorilor pentru stocarea mesajelor primite.

Programul de poștă electronică de pe un calculator, denumit **agent utilizator** (UA - *User Agent*) oferă utilizatorului o interfață spre sistemul de poștă electronică din Internet, care, în general, nu este considerată parte componentă a acestuia. Scopul UA este de a facilita accesul utilizatorului la serviciul de e-mail din rețea (Fig.II.11).

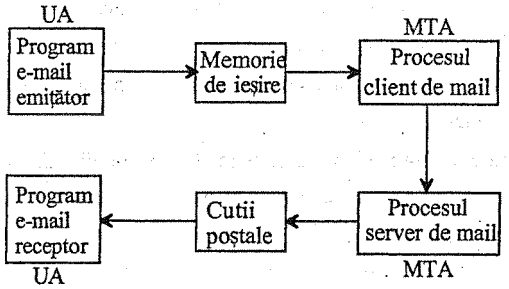


Fig. II.11 Structura sistemului de poștă electronică dintr-o rețea de calculatoare

Procesele (client sau server) care realizează serviciul de poștă electronică, prin transferul mesajelor în sau din Internet se numesc **agenți de transfer a mesajelor** (MTA - *Message Transfer Agent*). Între doi agenți de transfer a mesajelor se stabilește o conexiune TCP, iar comunicarea se face pe baza protocoalelor de poștă electronică (de exemplu, SMTP - *Simple Message Transfer Protocol*, POP - *Post-Office Protocol*).

Majoritatea MTA folosesc SMTP pentru transferul mesajelor în format NVT ASCII, prin conexiuni TCP la portul 25 (RFC 821).

SMTP permite comunicații duplex între client și server, pentru transmisia secvențelor de comandă în format NVT ASCII (Tabel II.5).

Tabel II.5

Comenzi ale protocolului SMTP

Comandă	Semnificație
HELO	identifică emițătorul SMTP față de receptorul SMTP (*hello*)
MAIL	inițiază o tranzacție de poștă (*mail*) către o cutie poștală
RCPT	recepționează datele la adresa specificată (*reception*)
DATA	avertizează receptorul că urmează să se transmită date
RSET	abanonează tranzacția poștală curentă (*reset*)
NOOP	a nu se efectua nici o operație și returnează mesajul OK (*no operation*)
QUIT	returnează OK și închide canalul de comunicație
VRFY	verifică dacă argumentul identifică un utilizator (*verify*)
SEND	distribuie datele unui terminal
SOML	transmite poșta unei cutii poștale sau unui terminal (*send or mail*)
SAML	transmite poșta unei cutii poștale și unui terminal (*send and mail*)
EXPN	furnizează în detaliu componența unei liste de mail (*expand*)
HELP	transmite informații ajutătoare emițătorului SMTP
TURN	solicită schimbarea rolurilor între transmițătorul și receptorul SMTP

Numai primele șapte comenzi din acest tabel sunt obligatorii, celelalte fiind opționale pentru implementările SMTP (RFC 1123).

Sintaxa comenzii MAIL (similară pentru SEND, SOML, SAML) este următoarea:

MAIL FROM: <cale inversa>

Argumentul < cale inversă> este dat prin adresa de e-mail a expeditorului.

Sintaxa comenzii de recepție RCPT este:

RCPT TO: <cale directa>

Argumentul < cale directă> se înlocuiește cu adresa de e-mail a destinatarului.

La orice comandă SMTP, serverul MTA transmite un cod de răspuns SMTP, eventual cu argument, cu semnificațiile date în tabelul II.6.

Observații

1. Se poate utiliza SMTP pentru transmisia mesajelor de tip text, dar și de altă natură (imagine, audio, video) prin definirea unor extensii ale protocolului.

2. SMTP este implicat în transmisia poștei electronice spre serverul de mail și spre Internet. Preluarea mesajelor de poștă de la cutiile poștale sau din Internet se face conform protocolului POP.

Tabel II.6

Coduri de răspuns SMTP

Cod	Semnificație
211	specifică starea sistemului sau este un răspuns la o comandă HELP
214	mesaj HELP
220	<domeniu> serviciu de poștă pregătit
221	<domeniu> serviciul închide canalul de comunicație
250	acțiune încheiată cu succes
251	nu există local acel utilizator; avans la <cale directa>
354	inițiază acțiunea de mail și se încheie cu <CRLF>
421	<domeniu> serviciul nu este disponibil; se închide canalul
450	cutie poștală nedisponibilă temporar
451	acțiune abandonată din cauza unei erori locale de prelucrare a datelor
452	acțiune ne finalizată din cauza memoriei insuficiente
500	eroare de sintaxă; comandă necunoscută
501	eroare de sintaxă a parametrilor sau argumentelor
502	comandă neimplementată
503	secvență incorectă de comenzi
504	parametru meimplementat
550	cutie poștală invalidă
551	nu există local acel utilizator; încearcă la <cale directă>
552	acțiune abandonată prin depășirea spațiului de stocare alocat
553	acțiune nefinalizată: numele cutiei poștale inexistent
554	tranzacție de poștă eșuată

Aceste coduri sunt formate din trei cifre, fiecare dintre acestea având o anumită semnificație.

Prima cifră poate fi:

1 MTA server acceptă comanda dar solicită clientului să confirme informația de răspuns.

2 MTA server a încheiat cu succes acțiunea solicitată și clientul poate iniția o nouă cerere.

3 MTA server acceptă comanda dar solicită furnizarea unor informații suplimentare.

4 MTA server nu acceptă comanda din cauza unei stări de eroare temporare. Clientul poate repeta comanda ulterior.

5 MTA server nu acceptă în mod categoric cererea clientului. Clientul nu trebuie să repete acea comandă decât dacă modifică argumentul sau parametrii.

A doua cifră indică:

0 eroare de sintaxă (comandă prea lungă sau neimplementată, argument invalid etc)

1 solicitarea de informații ajutătoare (*help*)

2 starea sistemului (pregătit sau nu, urmând să se închidă canalul)

3, 4 neutilizate în prezent

5 în mod exclusiv, acțiunea de mail (încheiată cu succes sau abandonată)

A treia cifră indică tipul textului descriptiv transmis după codul de răspuns.

Observații

1. În prezent, algoritmii SMTP nu acceptă ca prima cifră să fie 1, dar ea este definită în protocol pentru utilizări ulterioare.

2. Răspunsurile SMTP pot fi generate pe mai multe linii. În acest caz, este obligatoriu ca fiecare linie să înceapă cu codul 123 urmat de o cratimă și să se termine cu combinația de caractere CRLF. Numai pe ultima limie după codul de răspuns 123 nu mai apare acea cratimă, lipsa ei atenționând receptorul că este ultima linie din răspuns.

3. Pentru securizarea sistemului de e-mail, se poate configura serverul de mail să lucreze ca agent de comutație (*relay host*) sau hub de mail, astfel încât argumentele <cale directă> (*forward path*) și <cale inversă> (*reverse-path*) din comenzile SMTP adresate unei rețele să fie tocmai adresa acestui server. În comenzile MAIL și RCPT se poate impune calea ce o urmează un mesaj în rețea prin specificarea agenților de comutație, asemenea rutării pachetelor IP:

MAIL FROM: <@ HOST1, @HOST2, ... @HOSTn: adresa_cutiei_postale_de_destinatie>

În procesul de transmisie, la nivelul fiecărui agent de comutație, acesta șterge numele său din calea directă și îl adaugă în calea inversă. Astfel la hostul de destinație, calea directă conține numai adresa cutiei poștale locale.

SMTP impune anumite limite referitoare la lungimea maximă a șirurilor de caractere utilizate (Tabel II.7). De asemenea, SMTP poate gestiona maximum 100 de bufere de poștă electronică.

Tabel II.7

Lungimea maximă a șirurilor de caractere admisă de SMTP

Obiect SMTP	Lungime maximă (caractere)
Nume de utilizator	64
Domeniu	64
Cale	256
Linie de comandă	512
Linie de răspuns	512
Text descriptiv	1000

Exemplu: Tranzacție SMTP între utilizatorul "expeditor" din domeniul abc.ro, către un utilizator "destinatar" din domeniul xyz.ro:

1.	MTA SERVER	220 xyz.ro Simple Mai Transfer Service Ready
2.	MTA CLIENT	HELO abc.ro
3.	MTA SERVER	250 xyz.ro
4.	MTA CLIENT	MAIL FROM: <expeditor@abc.ro>
5.	MTA SERVER	250 OK
6.	MTA CLIENT	RCPT TO: < nume_eronat@xyz.ro>
7.	MTA SERVER	550 No such user here
8.	MTA CLIENT	RCPT TO: <destinatar@xyz.ro>
9.	MTA SERVER	250 OK
10.	MTA CLIENT	DATA
11.	MTA SERVER	354 Start mail input; end with <CRLF>. <CRLF>
12.	MTA CLIENT	123 - linia 1 din mesaj <CRLF>
13.	MTA CLIENT	123 linia 2 din mesaj <CRLF>
14.	MTA SERVER	250 OK
15.	MTA CLIENT	QUIT
16.	MTA SERVER	221 xyz.ro Service closing transmission channel

Orice mesaj de e-mail este compus din **antet** și **corp** (RFC 822). În antetul introdus de UA și transmis către MTA, în funcție de programul de e-mail folosit, pot să apară mai multe câmpuri (*Date, From, Subject, Reply-To, cc, Atachement, Comment, Message-ID, X-Special-Action* etc). La nivelul MTA se împachetează mesajul cu informații suplimentare (eventual se specifică o cale cu agenți de comutare) în așa-numita **anvelopă** și se transmite altui MTA sau agentului de comutare local.

Se pot defini extensii ale protocolului SMTP pentru transmisia prin sistemul de e-mail a unor documente de tip multimedia (RFC 1425, RFC 1427, RFC1521).

Protocolul MIME (*Multipurpose Internet Mail Extension*) reprezintă o extensie a SMTP. Acest protocol adaugă cinci noi câmpuri în antet, care permit transmisia prin atașare la mesajele de e-mail a textelor formatate (de exemplu, RTF - *Rich Text Format*), a imaginilor cu diverse formate (GIF - *Graphic Interchange Format,* JPEG - *Joint Photographic Experts Group*), a datelor în format binar sau PS (*Postscript*), a documentelor audio în format ISDN (*Integrated Services Digital Network*) cu lege de compandare μ și codare pe 8 biți precum și a fișierelor video în format MPEG (*Movie Photographic Experts Group*).

MIME prevede pe lângă formatul standard NVT ASCII pe 7 biți, diferite scheme de codare a caracterelor, utile pentru transmisii pe 8 biți, pentru criptarea datelor sau pentru transmisia unor caractere speciale, neincluse în setul ASCII:

Quoted -printable	pentru transmisia în format NVT-ASCII, a unei secvențe cu un număr mic de caractere având al 8-lea bit setat, fiecare dintre acestea fiind precedat de semnul 'egal' (=) (RFC 1522)
Base 64	codează 3 octeți ca 4 simboluri de 6 biți (RFC 1421)
8-bit	transmite caracterele (ASCII și non-ASCII) pe 8-biți
Binary	transmisie pe 8-biți fără caracterul sfârșit de linie.

Codarea *Base 64* se poate aplica oricărui fișier audio, video sau de imagine pentru a fi transmis prin e-mail, în format binar.

SMTP este responsabil de livrarea poștei electronice în Internet. Pentru preluarea mesajelor de e-mail din Internet se utilizează **protocolul POP,** orientat pe conexiunea dintre client și server.(Figura II.12).

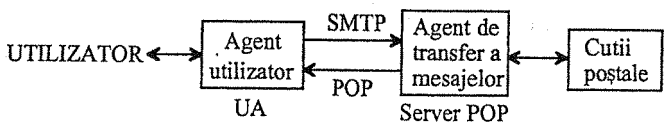


Fig. II.12 Configurația client-server POP

Deși oferă servicii relativ similare, versiunile POP2 (RFC 937) și POP3 (RFC 1225) sunt incompatibile și au asociate porturi de protocol diferite (109, 110).

POP2, corespondent fidel al SMTP, având comenzi asemănătoare, se aplică numai local.

Din motive de securitate, unii administratori de rețea dezactivează serviciul de acces de la distanță (*remote login*) în LAN.

Versiunea POP3 permite accesul de la distanță la serviciul de poștă electronică, mai precis la căsuța poștală rezervată utilizatorului.

O sesiune POP3 are trei stări: autorizare, tranzacție și actualizare (încheiere).

Pentru autorizarea accesului de la distanță la căsuța poștală a utilizatorului, aflată pe serverul POP3, protocolul prevede comenzi de identificare, cu nume de utilizator (USER) și parolă (PASS).

După autorizare, se poate efectua tranzacția, folosind comenzile:

STAT	Serverul informează clientul despre numărul de mesaje din cutia poștală și dimensiunea totală (*status*)
LIST	Afișează lista mesajelor (*listing*)
RETR	Preia un mesaj cu un anumit ID (*retrieve*)
DELE	Marchează un mesaj din cutia poștală pentru ștergere (*delete*)
RSET	Deselectează toate mesajele marcate pentru ștergere (*reset*)
LAST	Serverul returnează ID-ul ultimului mesaj accesat (*last message*)
NOOP	Serverul răspunde simplu (OK) fără a efectua vreo operație, comanda fiind utilă pentru testarea legăturii (*no operation*).

Închiderea sesiunii presupune ștergerea mesajelor și dezactivarea legăturii, cu comanda:

QUIT	Actualizează starea cutiei poștale și închide conexiunea TCP.

II.1.8 Protocoale pentru transferul fișierelor (FTP, TFTP, SFTP)

Serviciul de transfer a fișierelor în rețelele locale de calculatoare și în Internet se realizează pe baza protocoalelor de transfer a fișierelor, precum FTP (*File Transfer Protocol*), TFTP (*Trivial File Transfer Protocol*), SFTP (*Simple File Transfer Protocol*).

Protocoalele FTP (RFC 959) și SFTP (RFC 913) folosesc TCP pentru transport, ceea ce permite transferul sigur al datelor la destinație.

Protocolul TFTP (RFC 783) este implementat cu datagrame, pe baza UDP, astfel încât transferul devine nesigur, dar este simplu și rapid. TFTP este utilizat pentru transferul unor fișiere de mici dimensiuni.

Pentru transferul fișierelor în rețea, se poate utiliza și protocolul SSH (*Secure Shell Protocol*), cu cheie de criptare pentru securizarea transmisiei.

Protocolul FTP folosește coduri de comandă și de răspuns în formatul NVT ASCII, definit de Telnet, și două conexiuni TCP: **conexiunea de date** pentru transferul datelor și **conexiunea de control** pentru transmisia unor comenzi specifice.

Implementarea FTP se realizează pe baza modelului client-server în sisteme de operare diverse (UNIX, DOS, Windows), prin programe simple, de tip 'linie de comandă', sau complexe. cu interfață grafică de utilizator (GUI - *Graphic Unit Interface*) și structură de meniuri, comode din punctul de vedere al utilizatorilor.

Serverul FTP deschide o conexiune pasivă la portul de protocol 21, după care așteaptă cererile clienților.

O sesiune FTP se activează prin cererea clientului de stabilire a unei conexiuni TCP, la portul de protocol 21 al serverului, reprezentând **conexiunea de control**, activă pe toată durata comunicării.

Dacă serverul răspunde afirmativ, cu un cod de răspuns 220, se inițiază **faza de autentificare**, prin operația de *login*, cu validarea numelui de utilizator (cod de răspuns 331) și a parolei proprii (cod de răspuns 230).

După eventuala schimbare a directorului de lucru curent, pentru transferul datelor se deschid **conexiuni de date** separate pentru fiecare operație de transfer de fișiere, spre server (*upload*) sau dinspre server (*download*). Clientul comunică serverului numărul de port la care să se conecteze, prin comanda FTP PORT, și deschide o conexiune pasivă. Serverul activează conexiunea pe portul specificat de client. În această fază, clientul joacă rolul de server pe conexiunea de date. Spre deosebire de serverul FTP, care pe o conexiune pasivă acceptă accesul oricărui client, clientul FTP nu va accepta pe conexiunea pasivă inițiată de el decât accesul de la adresa serverului FTP cu care a comunicat.

Procesul de preluare de fișiere (*download*) se inițiază prin comanda RETR (*Retrieve*) iar cel de transfer a unui fișier pe server (*upload*) prin comanda de stocare STOR (*Store*). Închiderea unei sesiuni FTP se realizează prin comanda QUIT. Procesul de transfer al unui fișier poate fi întrerupt în orice moment la solicitarea clientului, în modul de date urgente.

Codul 220 de răspuns la serverului marchează stabilirea conexiunii de date.

Codul 550 semnifică blocarea accesului pe server (*Access denied*).

O configurație tipică FTP este reprezentată schematic în figura II.13.

Clientul și serverul utilizează fiecare câte o interfață de interpretare a protocoalelor (PI - *Protocol Interpreter*), între acestea fiind stabilită conexiunea de control pe toată durata transferului.

Transferul fișierului se realizează prin conexiunea de date care se stabilește între procesele FTP-client și FTP-server.

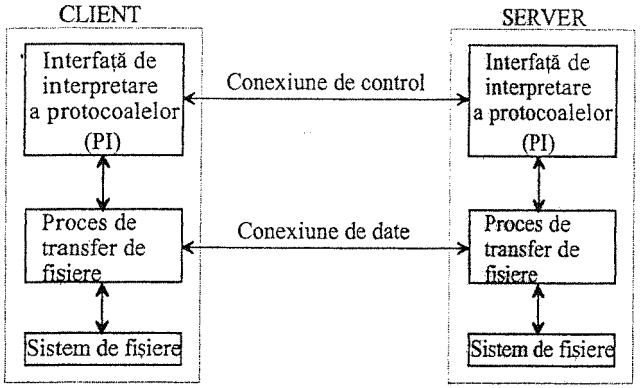


Fig. II.13 Schema de conexiuni FTP

Observații

1. Dacă un client nu dispune de un cont de utilizator pe un anumit server de fișiere, atunci se poate folosi FTP în varianta anonimă (*Anonymous FTP*), cu numele de utilizator *anonymous* și parola *guest*.

2. Asemenea protocoalelor de poștă electronică (SMTP, POP), FTP este un protocol de tip 'pas-cu-pas' (*lock step*), ceea ce înseamnă că după fiecare comandă lansată se așteaptă un răspuns și abia după primirea acestuia se transmite următoarea comandă.

3. FTP folosește Telnet pe conexiunea de control.

4. SFTP folosește o singură conexiune TCP și permite:

- validarea utilizatorilor pe baza listelor de control a accesului (ACL - *Access Control List*);
- transferul sigur al fișierelor;
- operații de listare, redenumire, ștergere de fișiere etc.

Totuși SFTP nu s-a impus.

5. Pe conexiunea de date se pot transfera fișiere între client și server, liste de directoare sau fișiere de pe server.

Protocolul FTP prevede peste 30 de comenzi, împărțite în trei categorii:

I. de control a accesului;

II. de negociere a parametrilor (opțiunilor);

III. de serviciu.

Comenzile FTP de control a accesului sunt următoarele:

USER {nume de utilizator}	- nume de utilizator (*user name*)
PASS {parola}	- parolă (*password*)
ACCT {nume/numar de cont}	- cont de utilizator (*account*)
CWD	- schimbarea directorului curent (*change working directory*)
CDUP	- trecere la directorul-părinte (*change to parent directory*)
SMNT	- stabilirea structurii de fișiere (*structure mount*)
REIN	- reinițializează programul-client (*reinitialise*), păstrând deschisă conexiunea de control pentru alți clienți
ABORT	- abandonarea transferului de fișiere
QUIT	- închiderea conexiunii.

Comenzile de negociere a parametrilor stabilesc opțiunile clientului. Protocolul FTP prevede patru **categorii de opțiuni**negociabile între client și server:

a. **tipuri de fișiere:**

local - transfer între calculatoare care folosesc cuvinte cu număr diferit de biți (L);

binar (imagine) - realizează transferul datelor din fișier ca flux de octeți (I);

EBCDIC (*Extended Binary Coded Decimal Interchange Code*) (E);

ASCII - tipul implicit pentru FTP, definit de Telnet pentru NVT (A).

b. **formate de fișiere:**

neprintabil (*nonprint*) - format implicit pentru FTP, care nu conține elemente de formatare verticală a textelor (N);

TELNET - folosește informația de control pentru formatare verticală;

FORTRAN - prevăzut cu caractere speciale de delimitare (CR - *Carriage Return*) în text (C).

c. **structuri de fișiere:**

structură tip "înregistrare" (R - *Record*) - sfârșitul înregistrării și al fișierului este marcat cu o combinație de două caractere;

structură tip "fișier" (F - *File*) - sfârșitul fișierului coincide cu închiderea conexiunii TCP;

structură tip "pagină" (P - *Page*).

d. **moduri de transmisie**

bloc - fișierele sunt transferate ca succesiuni de blocuri de date, cu antete proprii (B);

comprimat - fișierele sunt comprimate prin precodare RLL (*Run-Length Limited*) în vederea transferului (C);

flux de octeți (*stream*) - transferul fișierelor se face continuu, ca șir de octeți (S).

În general, FTP foloseste fișiere de tip binar sau ASCII, formatul neprintabil, structura de tip "fișier" și modul de transmisie ca flux de octeți.

Următoarele **comenzi de stabilire a opțiunilor** de transfer semnifică:

TYPE	- tipul fișierului;
STRU	- structura de fișiere (*structure*);
MODE	- modul de transfer;
PORT	- portul de date al cientului;
PASV	- clientul deschide o conexiune pasivă pe portul specificat.

Comenzi FTP de serviciu:

RETR	- preluare de fișier de pe alt calculator (*retrieve*);
STOR	- stocare de fișier pe alt calculator (*store*);
STOU	- stocare de fișier cu nume unic în director (*store unique*);
APPE	- adaugă date la un fișier aflat pe alt calculator (*append with create*);
ALLO	- alocă spațiu de memorie pe discul altui calculator (*allocate*);
REST	- reia procesul de transfer de date dintr-un fișier fără a retransmite datele deja transferate (*restart*);
ABOR	- abandonează procesul de transfer al unui fișier (*abort*);
DELE	- șterge un fișier de pe un alt calculator (*delete*);
LIST	- cere serverului lista fișierelor dintr-un director (*list*);
MKD	- creează un nou director pe alt calculator (*make directory*);
RMD	- șterge un director de pe alt calculator (*remove directory*);
SYST	- permite determinarea tipului sistemului de operare folosit pe alt calculator (*system*);
HELP	- clientul cere serverului informații ajutătoare referitoare la un argument (*help*);
NOOP	- testează conexiunea de control dintre client și server (*no operation*).

FTP folosește **coduri de răspuns** de trei cifre, asemenea SMTP, fiecare cifră având o anumită semnificație.

Prima cifră din codul de răspuns FTP semnifică tipul răspunsului serverului:

1 - preliminar pozitiv;

2 - definitiv pozitiv;

3 - intermediar pozitiv;

4 - temporar negativ;

5 - definitiv negativ.

Cea de a doua cifră reprezintă tipul textului care însoțește acel cod numeric de răspuns:

0 - eroare de sintaxă;

1 - informație;

2 - conexiuni;

3 - autentificare;

4 - nedefinit;

5 - sistem de fișiere.

A treia cifră din codul de răspuns FTP selectează textul descriptiv atașat acestuia, dintr-o listă de texte posibile.

Exemple de coduri de răspuns FTP:

125	conexiune de date deschisă; urmează transferul unui fișier
200	mesaj OK
220	serviciu pregătit pentru un nou client
230	numele și parola utilizatorului au fost validate; continuă
331	nume de utilizator validat; introdu parola
426	conexiune închisă; transfer abandonat
500	eroare de sintaxă; comandă necunoscută
502	comandă neimplementată
553	acțiune neexecutată; nume de fișier nepermis.

Comparativ cu FTP, **protocolul TFTP** utilizează un set restrâns de comenzi doar pentru scriereea sau citirea unui fișier, este mult mai simlu și poate fi folosit pentru transferul unor fișiere de dimensiuni mici, între echipamente interconectate direct (de exemplu, între două calculatoare sau între un calculator și un router).

Fișierele sunt transferate fragmentat, în datagrame cu lungime de 512 octeți, cu excepția ultimei care prin dimensiunea sa redusă marchează sfârșitul transmisiei.

Deoarece transportul datelor se face prin UDP și este nesigur, se impune aplicarea unor coduri de corecție a erorilor la nivelul antetului datagramei pentru a se găsi destinația corectă.

TFTP este utilizat și pentru transferul fișierelor de configurare (*boot*) din sistemul de operare, pe calculatoarele dintr-o rețea, la pornirea acestora (RFC 906). TFTP a devenit protocolul standard Internet pentru copierea programelor de boot pe stațiile de lucru fără disc, de pe un server de fișiere TFTP.

Protocolul SSH (*Secure Shell Protocol*) este un protocol utilizat pentru servicii de poștă electronică, transfer de fișiere și acces de la distanță, pe portul de aplicații 22, în baza modelului client-server, cu autentificarea utilizatorului și criptarea mesajelor. Acest protocol folosește algoritmi de criptare cu chei publice pentru clienți și server de 512 - 2048 biți, algoritmii DES (*Data Encryption System*) și 3DES (*Triple DES*). Este utilizat cu succes pentru transferul mesajelor între procesele de management din rețea.

II.1.9 Protocoale de timp pentru Internet

Pentru sincronizarea ceasurilor interne ale calculatoarelor conectate în rețea, se pot utiliza diferite protocoale de timp:

- NTP - *Network Time Protocol* (RFC 1305);
- SNTP - *Simple Network Time Protocol* (RFC 1361);
- *Daytime Protocol* (RFC 867);
- *Time Protocol* (RFC 868).

Aceste protocoale sunt rulate pe serverele de timp care, la cererea clientului, furnizează informații de timp, cu anumite precizii, folosind diferite referințe de timp.

De exemplu, PC-urile calculează timpul curent ca numărul de secunde scurse de la 1 ianuarie 1970, ora 00:00 GMT. În Internet, se ia ca referință data de 1 ianuarie 1990, ora 00:00 GMT. Momentele luate ca referințe de timp pot să creeze incompatibilități în procesele de comunicație din Internet.

Cunoașterea timpului în rețea este deosebit de utilă pentru majoritatea programelor rulate pe calculatoare, pentru determinarea duratelor unor procese de comunicație, datarea documentelor, calculul termenelor de expirare a licențelor, analiza statistică a tranferurilor de date etc.

Întrucât protocoalele de timp generează date numerice în format întreg, apar probleme legate de respectarea **ordinii octeților** în rețea și la nivelul calculatoarelor-gazdă.

În Internet, se transmite octetul mai semnificativ înaintea celui mai puțin semnificativ (ordinea *big indian*). Unele procesoare (Motorola, IBM, Macintosh) recunosc această ordine.

Alte procesoare, precum cele produse de firmele Intel și DEC (*Digital Equipment Corporation*), folosesc ordinea inversă (*little indian*), fiind necesară conversia formatului datelor la preluarea lor din Internet.

Protocolul *DAYTIME* generează informația de timp într-un format accesibil utilizatorului uman, precum:

<numele zilei><luna><ziua (numeric)><ora:minutul:secunda><anul>

Exemplu: Saturday, July 05, 10:23:30, 2003.

Șirul de caractere se încheie cu combinația CRLF specifică formatului NVT ASCII.

Protocolul *TIME* este unul dintre cele mai simple protocoale de timp folosite în Internet. Serverul *TIME* furnizează informația de timp curent ca număr de 4 octeți (*long integer*), reprezentând numărul de secunde scurse de la 1 ianuarie 1900, ora 12:00:01 AM până în prezent. Prin urmare, apare o diferență de 70 de ani față de referința de timp utilizată de un server Internet. Aceasta corespunde valorii hexazecimale exprimate ca întreg fără semn 0x.83.AA.7E.80.

Observație

În literatura de specialitate, există convenția ca toate valorile hexazecimale să fie precedate de prefixul '0x', care nu se ia în considerare în calculul lungimii întregului ca număr de octeți. De exemplu, 0x.23 reprezintă un singur octet (23) exprimat în format hexazecimal.

Comunicația dintre clientul și serverul *TIME* se realizează în mai mulți pași:

Pas 1. Serverul de timp 'ascultă' portul de aplicații 37 în așteptarea cererii unui client, transmisă fie prin TCP, fie prin UDP.

Pas 2. Dacă un client deschide o conexiune la portul 37 sau serverul recepționează o datagramă vidă pe acest port, atunci serverul de timp trimite clientului informația privind data și ora curentă, sub forma unui număr de 32 de biți, fie prin TCP după care închide conexiunea, fie printr-o datagramă UDP.

Pas 3. Clientul *TIME* recepționează datele și, în cazul utilizării TCP, închide conexiunea.

Protocoalele *DAYTIME* (portul 13) și *TIME* (portul 37) pot lucra atât cu TCP, cât și cu UDP.

NTP, dezvoltat din protocolul *TIME*, în mai multe versiuni (RFC 958, RFC 1305), corespunde portului de protocol 123 și este cel mai complex dintre protocoalele de timp utilizate în Internet, având o precizie de 1 - 50 milisecunde față de timpul standard oficial. Folosește UDP ca protocol de transport, IP cu sume de control Internet și ICMP (RFC 792) pentru transmisia mesajelor de interogare privind informația de timp (*timestamp message*).

SNTP utilizează algoritmi simplificați față de NTP, care nu asigură aceeași precizie de generare a informațiilor de timp.

În Internet, se utilizează o structură ierarhică de servere NTP. Serverele primare generează informația de timp cu precizie maximă și se interoghează reciproc, periodic, pentru sincronizare. Serverele NTP secundare își sincronizează ceasul prin cereri periodice adresate serverelor primare de timp. Serverele secundare furnizează clienților informații de timp mai puțin precise din cauza erorilor care apar în procesul de comunicație.

Este necesar ca între oricare două calculatoare (servere sau hosturi) care comunică în rețea prin protocoale de timp, să se procedeze la sincronizarea periodică a ceasurilor interne, în pereche.

Observație

Este dificilă estimarea cu precizie a duratei de transfer în rețea a pachetelor IP de la sursă la destinație, chiar dacă se folosește NTP. Operația este necesară pentru analiza statistică a proceselor de comunicație care se desfășoară în rețea.

II.1.10 Protocolul ICMP

Protocolul ICMP (*Internet Control Message Protocol*) corespunde nivelului Internet din modelul TCP/IP, fiind responsabil de transmisia mesajelor de eroare sau de interogare, utile pentru procesele de comunicație din rețea, dar și pentru testarea și depanarea acesteia.

Aplicațiile comunică direct cu ICMP și nu prin intermediul protocoalelor de transport.

Pentru încapsularea mesajelor și transmisia lor în rețea sub formă de pachete, ICMP folosește protocolul Internet.

Protocolul ICMP are unele limitări:

1. Raportează eroarea de transmisie a unui pachet numai sursei.

2. Nu transmite mesaje de eroare asociate altor mesaje ICMP.

3. Nu generează mesaje pe adrese de destinație de tip 'broadcast' sau 'multicast', pentru a evita încărcarea rețelei prin apariția fenomenelor de "furtună-în-rețea" (*broadcast storm*).

4. Nu furnizează mesaje de eroare pentru toate fragmentele unei datagrame eronate, ci numai pentru primul.

ICMP folosește 15 tipuri de mesaje. În general, modulele software care implementează ICMP nu includ decât anumite mesaje (Tabel II.8).

Împachetarea mesajelor ICMP se face cu un antet de 4 octeți, în care se specifică tipul mesajului, codul de răspuns și suma de control Internet (Fig. II.14).

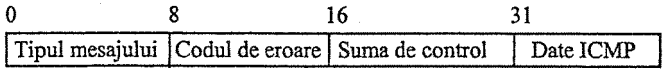


Fig. II.14 Formatul mesajului ICMP

Tabel II.8

Mesaje ICMP

Tip	Semnificație
0	Răspuns la ecou (*Echo Reply*)
3	Destinație inaccesibilă (*Destination Unreachable*)
5	Redirecționare (*Redirect*)
8	Cerere de ecou (*Echo Request*)
9	Informație de rutare (*Router Reply*)
10	Cerere de rutare (*Router Request*)
11	Timpul de viață a expirat (*Time-to-Live Expired*)
13	Cerere de sincronizare a ceasului (*Timestamp Request*)
14	Răspuns de sincronizare a ceasului (*Timestamp Reply*)
17	Cerere pentru masca de rețea (*Network Mask Request*)
18	Furnizarea măștii de rețea (*Network Mask Reply*)

Lungimea și conținutul câmpului de date ICMP depind de tipul mesajului.

Pentru mesaje de eroare, în acest câmp se transmit primii 64 de octeți din pachetul IP care a provocat eroarea.

Pentru mesaje de interogare de tip 'ecou' (0), folosite pentru testarea conexiunilor de către aplicația PING (*Packet INternet Groper*), câmpul de date ICMP include un octet de identificare, un octet 'număr de secvență' și alți doi octeți reprezentând o secvență opțională de date.

Câmpul de date din mesajele ICMP de tip 3, "destinație inaccesibilă", conține 68 de octeți, dintre care primii patru corespund unui cuvânt de 32 de biți complet nul iar următorii 64 de octeți provin din pachetul original transmis.

Similar, pentru mesajele de redirecționare, se includ în câmpul datelor adresa IP a routerului (*next hop*) și primii 64 de octeți din pachet.

Stațiile de lucru fără disc folosesc ICMP pentru aflarea propriei măști de rețea. Mesajele ICMP de cerere și răspuns referitoare la aceasta, includ în câmpul datelor ICMP de 8 octeți, un identificator și un număr de secvență, urmate de masca de rețea propriu-zisă.

Observații

1. Suma de control Internet calculată pe 16 biți (RFC 1071) se aplică atât antetului ICMP, cât și câmpului de date.

2. La același tip de mesaj, se pot asocia coduri de răspuns diferite în funcție de cauza problemei. De exemplu, pentru destinație inaccesibilă sunt posibile 16 coduri de răspuns (rețea inaccesibilă, protocol inaccesibil, rețea de destinație necunoscută etc).

3. Mesajul ICMP este încapsulat în vederea transmisiei cu antetul IP.

4. Operația PING se realizează în două faze: prima de transmisie a cererii de ecou ICMP, a doua de recepționare a răspunsului la ecou prin intermediul ICMP. Un răspuns afirmativ, de găsire a destinației, include durata de transfer dus-întors a pachetului între sursă și destinație, exprimată în milisecunde, rata de erori etc.

5. Mesajele ICMP de interogare a routerelor sunt utilizate pentru actualizarea dinamică a tabelelor de rutare.

II.1.11 Protocoale de management a rețelei

Gestionarea rețelelor de calculatoare se realizează pe baza protocoalelor de management de rețea.

- Suita TCP/IP include protocolul de management SNMP (*Simple Network Management Protocol*) definit în RFC 1155 - 1157, care implementează un mecanism de gestionare a resurselor rețelei, folosind baze de date MIB (*Management Information Base*), cu informații referitoare la toate componentele rețelei (RFC 1514 - *Host Resources MIB;* RFC 1398 - *Ethernet-like Interface Types MIB;* RFC 1493 - *Bridge MIB* și altele). RFC 1213 definește MIB-II care include obiectele gestionate pentru rețelele bazate pe suita TCP/IP.

SNMP poate folosi oricare din protocoalele de transport din suita TCP/IP dar în cele mai multe cazuri utilizează UDP, pe porturile de aplicații 161 și 162.

Un sistem de management a rețelelor de calculatoare include trei categorii de componente (Fig. II.15):

1. **componente gestionate** (*managed device*);
2. **stații de gestionare sau de management** (*network management station*);
3. **protocolul de management** (*management protocol*) utilizat pentru comunicația dintre celelalte componente ale sistemului de management.

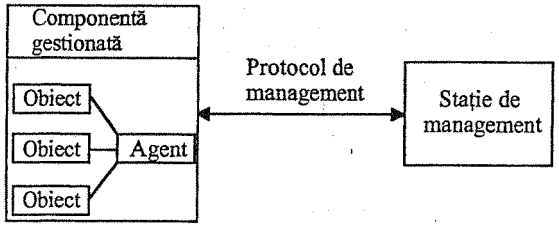


Fig.II.15 Structura de bază a sistemului de management al rețelei

RFC 1155 descrie un mecanism de identificare și descriere a obiectelor din MIB, denumit SMI (*Structure of Management Information*), care definește schema de organizare a colecției de obiecte gestionate din MIB, pe baza unei diagrame 'arbore', cu mai multe nivele (Fig.II.16).

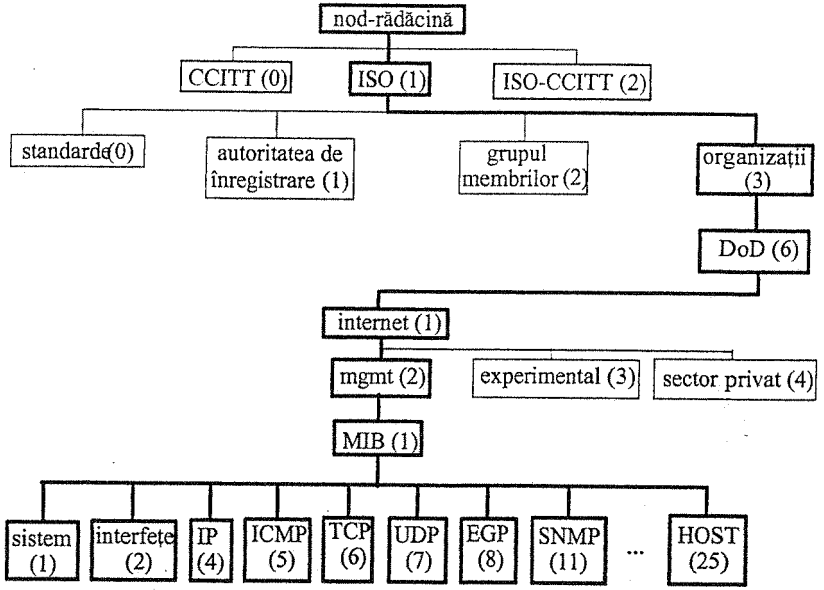


Fig. II.16 Diagrama-arbore de organizare a MIB în Internet

Fiecare nod din această diagramă este numerotat și, eventual, i se asociază și un scurt text descriptiv.

Observăm că în MIB I sunt incluse ca obiecte protocoalele din suita TCP/IP (în figură au fost reprezentate doar câteva dintre acestea).

Referitor la fiecare obiect, în MIB sunt incluse informații de natură administrativă și operațională.

Fiecare obiect se specifică numele, sintaxa, modul de acces, starea și o descriere a acestuia.

Numele reprezintă un identificator global, unic al obiectului, care rezultă urmărind calea care leagă nodul-rădăcină și obiectul gestionat din MIB. Acesta poate fi exprimat în trei formate diferite, echivalente:

1. **numeric cu puncte;**
2. **text** cu separare prin puncte, încadrat de paranteze pătrate;
3. **combinat** (text și numere de noduri).

De exemplu, pentru protocolul IP se specifică numele sau identificatorul:

1.3.6.1.2.1.4

echivalent cu:

[iso org dod internet mgmt mib 4]

echivalent cu

[iso(1) org(3) dod(6) internet(1) mgmt(2) mib(1) 4].

Se poate utiliza și un nume relativ, de exemplu [mib 4], care specifică al 4-lea nod din sub-arborele "MIB".

Nu se impun limite referitor la lungimea șirului de caractere care identifică un obiect din MIB.

Fiecărui obiect din MIB i se asociază un șir de caractere pentru descrierea sa, un așa-numit **mnemonic**, mai comod pentru utilizatorul uman decât un nume exprimat numeric (de exemplu, *sysDescr* pentru nodul "sistem" sau *ifTable* pentru nodul "interfețe" etc).

De fapt, obiectele din MIB sunt manipulate pe baza unor valori memorate la diverse momente (*instances*), ca date de tipuri diferite în funcție de natura obiectului.

Stațiile de management a rețelelor (NMS - *Network Management Station*) lucrează cu aceste valori instantanee ale obiectelor care sunt identificate prin așa-numitul **identificator de valoare** (*instance-identifier*), atașat identificatorului de obiect.

Dacă obiectul nu este o coloană dintr-un tabel, se folosește identificatorul de valoare 'nul' (0).

Exemplu: Se utilizează *sysDescr*.0 echivalent cu 1.3.6.1.2.1.1.0 pentru obiectul 'sistem'.

Dacă obiectul gestionat din MIB este structurat ca o coloană dintr-un tabel, atunci se anexează la identificatorul de obiect, indicii corespunzători coloanei din acel tabel, mai precis celulei în care este înregistrată o anumită valoare. În caz general, se anexează indicii tuturor coloanelor care descriu obiectul analizat.

Exemplu: Pentru starea unei conexiuni TCP (*tcpConnState*) specificată prin identificatorul relativ la TCP, 13.1.1, se combină în identificatorul de valoare adresa IP a sursei (192.168.34.81), portul de aplicație sursă (23), adresa IP a destinației (194.210.225.14), portul de aplicație de la destinație (2002) și se anexează identificatorului de obiect, rezultând:

1.3.6.1.2.1.6.13.1.1.192.168.34.81.23.194.210.225.14.2002

Sintaxa unui obiect constă în tipul datelor referitoare la acesta (INTEGER, OCTET STRING ș.a.).

Accesul la un obiect din MIB poate fi restricționat (*not-accessible; read-only; write-only*) sau liber (*read-write*).

Prin **starea** unui obiect se exprimă condițiile de implementare ale acestuia:

1. **mandatar**: componenta gestionată de NMS implementează în mod obligatoriu acel obiect;

2. **opțional**: componenta gestionată de NMS implementează opțional acel obiect;

3. **depășit:** componenta gestionată de NMS nu mai implementează acel obiect;

4. **depreciat**: componenta gestionată de NMS poate implementa acel obiect, dar există un nou obiect în MIB superior acestuia.

Descrierea obiectului se poate face printr-un scurt text descriptiv asociat acestuia.

Protocolul SNMP este utilizat de stația de management (NMS) pentru a transmite mesaje componentei gestionate, mai precis agentului de management din cadrul acesteia.

În general, SNMP acționează în mod recursiv, prin interogarea periodică (*polling*) a agenților de management ai componentelor gestionate de NMS.

Numai în situații critice, un agent poate iniția schimbul de informații cu NMS, pentru a o înștiința de modificările apărute, transmițând mesaje-capcană (*trap*) care întrerup procesul de *polling*. Un agent nu poate transmite oricât de multe mesaje-capcană spre NMS, pentru a evita pierderea controlului asupra întregii rețele.

Un mesaj SNMP (figura II.17) include un câmp de versiune a protocolului, un câmp referitor la grupul de utilizatori cărora li se adresează mesajul și un câmp de date.

Versiune	Grup adresabil	Date

Fig. II.17 Formatul mesajului SNMP

Prin stabilirea adresabilității protocolului, se realizează o procedură simplă de autentificare a mesajelor.

Unitatea de date sau mesajul SNMP (PDU - *Protocol Data Unit*) poate fi denumită în cinci moduri distincte, în funcție de natura informației transmise:

1. **cerere simplă** (*get-request*) - NMS cere unui agent de management informații despre un obiect;

2. **cerere recursivă** (*get-next-request*) - NMS cere unui agent de management informații despre obiectul următor din MIB;

3. **cerere de impunere** (*set-request*) - NMS impune o anumită valoare pentru un obiect din MIB-ul agentului;

4. **răspuns** (*get-response*) - un agent trimite informații spre NMS, despre un obiect, ca răspuns la cererea acesteia;

5. **"capcană"** (*trap*) - un agent transmite spre MIB informații referitoare la un eveniment extraordinar care a afectat componenta gestionată prin intermediul său (reinițializarea agentului de management, schimbarea stării unei interfețe, nerespectarea unor condiții de autentificare etc). Există sapte tipuri de mesaje-capcană SNMP.

Primele patru tipuri de mesaje SNMP se transmit prin UDP, pe portul 161. Numai mesajele-capcană se transmit pe portul de aplicație 162.

SNMP este considerat a fi un protocol simplu deoarece nu are decât cinci operații, corespunzătoare celor cinci tipuri de mesaje SNMP (*get, get-next, set, get-response* și *trap*).

În funcție de modul de acces, se poate folosi un număr mai mic de mesaje SNMP.

Obiectele din MIB pot fi grupate în subseturi (SNMP MIB *View*), în funcție de accesibilitatea acestora: parțială (*read-only*) sau totală (*read-write*).

Pentru agenții de management, se definesc **profile** prin care se stabilesc drepturile de acces la diferitele subseturi de obiecte din MIB, total sau parțial accesibile (Tabel II.9):

1. cu drept de citire (*read-only*);
2. cu drept de scriere (*write-only*);
3. cu drepturi de citire și de scriere (*read-write*);
4. fără drepturi de acces la MIB (*not-accessible*).

Tabel II.9

Operații SNMP admise profilelor de agenți

în funcție de accesibilitatea obiectelor din MIB

Accesibilitatea obiectului SNMP	Profilele agenților de management			
	cu drept de citire	cu drept de scriere	cu drepturi de citire și de scriere	fără drepturi de acces
parțială	cerere simplă cerere recursivă cerere-capcană	-	cerere simplă cerere recursivă cerere-capcană	-
totală	cerere simplă cerere recursivă cerere-capcană	cerere simplă cerere recursivă cerere de impunere cerere-capcană	cerere simplă cerere recursivă cerere de impunere cerere-capcană	-

Observații

1. Se impun măsuri stricte de securitate referitor la mesajele SNMP, întrucât prin definirea unui profil de agenți cu drept de scriere pe un grup de obiecte cu accesibilitate totală se pot produce daune majore rețelei de către persoane neautorizate care cunosc numele profilului.

2. SNMP este un protocol rutabil întrucât folosește protocolul IP pentru încapsularea datelor și, implicit, adresarea IP.

3. Există și protocoale de management al rețelelor locale de calculatoare, nerutabile. Un astfel de protocol este NetBeui (*Network BIOS extended user interface*), dezvoltat de firma Microsoft pentru rețele Netware (de PC-uri), cu sistem de operare NT, pe baza modelului client-server. Pe lângă operațiile de management de rețea, NetBeui include și funcțiile de transport, de corecție a erorilor de transmisie, de confirmare a recepției corecte a datelor (ACK), fiind echivalent unei stive de protocoale cu funcții distincte. Toate acestea determină o creștere considerabilă a timpului de transmisie a pachetelor și apariția blocajelor în rețea cauzate de așteptarea unor mesaje de confirmare pierdute. O altă limitare a NetBeui este aceea dată de numărul maxim admis de sesiuni simultan deschise în rețea (254). Aceste dezavantaje ale NetBeui sunt eliminate în cadrul protocolului NBF (*NetBeui Frame*), cu 'fereastră glisantă' de transmisie (*sliding window*).

II.1.12 Protocoale de securitate în Internet

Securitatea comunicațiilor în rețelele locale de calculatoare se referă la mai multe aspecte:

1. mesajele transmise provin din surse autorizate și sunt autentice;
2. datele sunt corecte și complete;
3. accesul la anumite mesaje cu caracter confidențial este restricționat în mod corespunzător.

Există diferite metode de asigurare a securității transmisiei într-o rețea prin operații de autentificare a utilizatorilor, criptare a mesajelor, filtrare a traficului etc.

Metodele de securitate din Internet se pot aplica pe diferite nivele ale modelului OSI.

La nivel fizic, se pot folosi module hardware de criptare și decriptare (ENCO).

La nivelul legăturii de date și la nivel de rețea se pot defini filtre de includere sau de excludere pe diverse interfețe ale echipamentelor.

Se pot utiliza programe de aplicație specializate pentru asigurarea securității transmisiei datelor în rețea.

Primele măsuri de securitate a rețelelor defineau **asociații de securitate** (SA - *Security Association*), adică grupuri de utilizatori autorizați să folosească o anumită rețea, denumită **rețea virtuală privată** (VPN - *Virtual Private Network*).

În prezent, în rețelele TCP/IP se utilizează suita de protocoale de securitate **IPsec** (*Internet Protocol Security Facility*), care realizează criptarea și autentificarea pachetelor IP cu performanțe

superioare sistemului inițial SA. VPN pot fi configurate în mod adecvat să aplice protocoalele de securitate din suita IPsec.

Gradul de protecție a pachetelor IP și cheile de criptare utilizate de IPsec se stabilesc prin mecanismul IKE (*Internet Key Exchange*), care se aplică folosind protocolul ISAKMP (*Internet Security Association and Key Management Protocol*). Astfel IPsec beneficiază de serviciile ISAKMP/IKE.

IPsec oferă următoarele servicii de securitate pe nivelul IP al rețelelor TCP/IP:

1. **integritatea conexiunii** - asigură faptul că în procesul de comunicație nu intervin entități neautorizate care să modifice datele sau să genereze mesaje false în rețea;

2. **autentificarea sursei de date** - permite identificarea sursei și asigurarea autenticității mesajelor;

3. **criptarea datelor** - asigură confidențialitatea mesajelor transmise și imposibilitatea preluării neautorizate a informațiilor;

4. **protecția la atacuri în rețea** - detectează pachetele repetitive, replici ale aceluiași pachet, care se transmit la infinit în rețea și pot produce blocaje sau saturarea rețelei (*flooding*).

Autentificarea sursei se face pe baza protocolului AH (*IP Authentication Header*) din suita IPsec (RFC 2401, RFC 2402). Acest protocol asigură integritatea conexiunii și a datelor transmise, precum și autenticitatea mesajelor. AH asigură securitatea integrală a pachetelor IP, inclusiv antetelor de securitate atașate ulterior acestora.

Serviciile de securitate sunt asigurate și de protocolul ESP de încapsulare a pachetelor IP (*IP Encapsulating Security Payload*), care stabilește operații de criptare a datelor și de autentificare a sursei de informații (RFC 2406).

ESP oferă servicii de securitate numai protocoalelor de pe nivelele superioare celui de rețea, excluzând antetele de securitate ulterior adăugate pachetelor.

Protocoalele AH și ESP pot fi implementate prin diverși algoritmi software și se pot aplica fie individual, fie ambele simultan, în funcție de gradul de securitate impus pachetelor IP (RFC 2403, RFC 2404).

IPsec asigură securitatea comunicației dintre două calculatoare-gazdă, dintre două echipamente de comunicații (de exemplu, rutere) sau dintre un DTE și un DCE.

Un router sau un server pe care sunt activate protocoalele de securitate IPsec se numește **poartă de securitate** (*security gateway*) sau **"zid" de protecție** (*firewall*).

În general, asigurarea securității unei transmisii se realizează la ambele capete ale căii de comunicație, cu două echipamente care folosesc IPsec lucrând în pereche (*IPsec peers*).

Cele două protocoale de securitate în Internet (AH sau ESP) pot acționa în două moduri:

1. **modul de transport** - protocolul de securitate intervine în pachetul IP și adaugă un ante de securitate imediat după antetul IP (cu sau fără opțiuni exprimate). ESP oferă protecție numa protocoalelor de nivel superior, în timp ce AH securizează total pachetul, inclusiv antetul IP.

2. **modul de tunelare** (*IP tunneling*) - se introduc două antete de securitate în fiecar pachet, înainte (*outer header*) și după (*inner header*) antetul IP. Antetul extern specifică pereche de entități între care se creează tunelul IP și se aplică măsurile de securitate pe baza IPsec. Antetu intern precizează destinația finală a pachetului. ESP protejează numai pachetul transmis prin tunelu IP, în timp ce AH asigură și securitatea antetului exterior atașat.

Configurarea echipamentelor dintr-o rețea în vederea aplicării IPsec se realizează de către o persoană cu drepturi depline de stabilire a securității rețelei (*security officer*), în trei etape:

1. crearea grupurilor de securitate (SA) și stabilirea drepturilor și atribuțiilor acestora;

2. configurarea legăturilor dintre SA-uri și stabilirea ierarhiilor de priorități, folosind ISAKMP/IKE (RFC 2408, RFC 2409);

3. stabilirea modalităților de clasificare a pachetelor IP și de acțiune asupra lor (permite sau interzice accesul în rețea, aplică procedurile de securitate conform IPsec).

Aceste configurații referitoare la IPsec sunt stocate în bazele de date pentru securitatea rețelei (SPD - *Security Policy Database*), la care are acces doar administratorul de rețea.

Prin SA înțelegem o conexiune simplex definită pe o pereche IPsec, pentru securitatea traficului doar într-un sens, folosind un singur protocol de securitate (AH sau ESP).

Pentru transmisiile duplex se definește câte un SA pentru fiecare sens de comunicație cu rețeaua (*inbound/outbound traffic*).

Dacă la unul din capetele canalului de comunicație definit de SA, se găsește un echipament de securitate (*security gateway; firewall*), atunci este obligatoriu ca acel SA să lucreze în modul de tunelare pentru a evita problemele create prin fragmentarea pachetelor și de existența căilor multiple de rutare.

Un SA este identificat prin trei parametri:

1. un număr aleator denumit **identificator de securitate** (SPI - *Security Parameter Index*);

2. **adresa IP de destinație;**

3. **protocolul de securitate** (AH sau ESP).

Dacă este necesară utilizarea ambelor protocoale de securitate în Internet (AH și ESP), atunci se creează și se configurează legăturile dintre două sau mai multe SA.

Regulile de securitate aplicate într-o rețea folosind IPsec sunt memorate în SPD. Acestea stabilesc trei moduri posibile de acțiune asupra pachetelor IP:

1. se aplică pachetului, serviciile de securitate conform IPsec;

2. se interzice accesul pachetului în rețea (*deny*);

3. se acordă permisiunea de acces în rețea, fără aplicarea măsurilor de securitate IP (*bypass IPsec*).

Modul de acțiune asupra unui pachet IP se stabilește pe baza antetelor conținute de acesta, prin operația de clasificare a pachetelor, în funcție de diverși **factori de selecție**:

- adresa IP a sursei;
- adresa IP a destinației;
- portul-sursă;
- portul-destinație;
- protocolul de transport;
- numele utilizatorului sau al sistemului;
- gradul de prioritate a informațiilor conținute în pachet.

Aplicarea măsurilor de securitate IPsec asupra unui pachet (autentificare, criptare, compresie), se realizează pe baza mecanismului ISAKMP/IKE prin care se generează și se transmit între părți cheile de criptare utilizate de SA în diferite sesiuni, memorate într-o bază de date proprie ISAKMP ca atribute ale SA.

În rețelele TCP/IP, se utilizeazează diverși algoritmi de criptare, uzuali fiind cei cu cheie publică (RSA, Diffie-Hellman, DES, 3DES etc).

De exemplu, protocolul SSH, utilizat pentru transferul securizat al fișierelor și al mesajelor prin sistemul de poștă electronică din Internet, folosește diverși algoritmi de criptare cu cheie publică. Operația de autentificare se bazează de asemenea pe secvențe de tip 'cheie de transmisie'.

APLICAȚII

1. Încărcați de pe Internet și analizați cele mai recente documente RFC referitoare la protocoalele din suita TCP/IP.
2. Lansați în execuție diferite programe de aplicații de tip poștă-electronică și de transfer a fișierelor. Observați performanțele fiecăruia.
3. Aplicați diferite comenzi specifice protocoalelor din suita TCP/IP și observați efectele acestora precum și codurile de răspuns generate.
4. Studiați algoritmii de criptare a datelor în Internet (DES, IDEA, RSA) și faceți o comparație a performanțelor acestora.
5. Testați conexiunile dintre diferite noduri din rețeaua locală, eventual și din Internet.
6. Deduceți rutele de acces dintre diverse servere din Internet.

II.2 Suita de protocoale Novell IPX/SPX

Suita de protocoale de comunicații IPX/SPX (*Internetwork Packet eXchange / Sequenced Packet eXchange*) se utilizează în rețelele de calculatoare Novell (Netware), pe baza modelului client/server.

IPX (*Internetwork Packet eXchange*) este un protocol de nivel OSI 3 (rețea), fără conexiune, care încapsulează datele în **datagrame**. Aceste protocol a fost dezvoltat pe baza protocolului XNS (*Xerox Network Standard*) creat de corporația Xerox. În fapt, XNS desemnează o suită de protocoale de comunicație echivalentă cu TCP/IP, dar care folosește forme diferite de pachete și terminologie distinctă față de aceasta. IPX nu prevede operații de detecție a erorilor de transmisie și nici transmisia mesajelor de confirmare (ACK) în cazul recepției corecte a pachetelor.

SPX (*Sequenced Packet eXchange*) este protocolul de transport, orientat pe conexiune, care utilizează un circuit virtual de comunicație între sursă și destinație. Acest protocol folosește câmpuri de detecție a erorilor de transmisie, mesaje de confirmare a recepției corecte precum și numere de secvențe în cazul fragmentării mesajelor în mai multe pachete IPX, în vederea reasamblării lor corecte la recepție. SPX realizează și un control al fluxului informațional pentru evitarea pierderii datelor prin supraîncărcarea memoriilor-tampon (*buffer*) din rețea.

Din suita IPX/SPX mai fac parte și alte protocoale care nu pot fi clasificate pe baza modelului OSI, dar sunt echivalente nivelelor superioare din modelul OSI, comparativ cu IPX:

- protocolul de rutare RIP (*Routing Information Protocol*);
- protocolul de servicii SAP (*Service Advertising Protocol*);
- protocolul de control NCP (*NetWare Core Protocol*).

Protocolul IPX încapsulează datele de pe nivelele superioare cu un antet de 30 de octeți, în datagrame cu lungime maximă de 576 de octeți (Fig. II.18).

Sumă de control 2B	Lungimea pachetului 2B	TTL 1B	Tip 1B	Adresa de destinație 12 B	Adresa sursei 12B	Date maximum 546 B

Antet IPX (30 B)

Fig. II.18 Structura pachetului de date IPX

IPX nu calculează nici o sumă de control, primul câmp fiind practic neutilizat.

Lungimea pachetului IPX se exprimă în octeți, pe 16 biți.

Timpul de viață al pachetului (TTL - *Time to Live*) este decrementat la trecerea printr-un ruter iar în momentul în care acest timp expiră, pachetul IPX este automat distrus.

Tipul pachetului semnifică protocolul de nivel superior care a generat datele (SPX, RIP, NCP, SAP).

Câmpurile de adrese (sursă și destinație) sunt structurate pe principiul **adresării IPX** cu:

- **identificator de rețea** (N - *Network*) de 4 octeți;
- **identificatorul calculatorului-gazdă** (H - *Host*) - de 6 octeți;
- **identificatorul de aplicație** (S - *Socket*) - de 2 octeți.

Adresele IPX sunt ordonate ierarhic asemenea adreselor IP, dar spre deosebire de acestea includ un segment suplimentar care identifică aplicațiile sursă și destinație, prin zonele de memorie rezervate acestora (*socket*). IPX admite cel mult 50 de socketuri pe un calculator. Anumite protocoale de nivel superior (RIP, SAP, NCP, NetBIOS) au numere de port rezervate.

Protocolul de transport SPX din suita IPX/SPX încapsulează mesajele generate de programele de aplicație în **pachete SPX**, cu un antet de 12 octeți și lungime maximă a pachetului de 546 de octeți (Fig. II.19).

Controlul conexiunii 1B	Tipul datelor 1B	ID socket sursă 2B	ID socket destinație 2B	Număr de secvență 2B	Număr de confirmare 2B	Controlul fluxului 2B	Date max.534 B

← Antet SPX (12 B) →

Fig. II.19 Structura pachetului SPX

Protocolul SAP este utilizat de serverele din rețea pentru a informa celelalte servere din rețea, prin mesaje transmise periodic în modul broadcast, asupra serviciilor pe care le oferă. În general, aceste mesaje SAP se reiau la fiecare 60 de secunde. SAP poate fi utilizat de către clienți pentru a obține informații despre un server din rețea.

Orice calculator din rețea poate deveni client SAP, prin interogarea serverului cu un pachet SAP, încapsulat de IPX.

În pachetul SAP sunt incluse operația efectuată (transmisie broadcast sau cerere de informare) și informații despre servere (maximum 7): tipul serverului (2B), numele serverului (48B), adresa sa IPX (12B), numărul de noduri intermediare (*hops*) (2B).

Tipul serverului este specificat printr-un cod valoric (Tabelul II.10).

Numărul de noduri precizează distanța dintre serverul local și alt server care oferă un anumit serviciu.

Protocolul NCP stabilește un set de comenzi prin intermediul cărora se transmit cererile de serviciu și răspunsurile între clienții și serverele dintr-o rețea Netware. NCP este similar sistemului NetBIOS folosit în rețelele locale cu sistem de operare DOS.

Mesajele NCP sunt împachetate într-un pachet NCP de maximum 546 octeți, cu un antet

NCP de 7 octeți în care se specifică: tipul cererii (2B), numărul de secvență (1B), număru conexiunii (1B), numărul programului prin care se efectuează serviciul respectiv (1B), un câmp rezervat de un octet și un cod al funcției îndeplinite (1B).

Tabelul II.10

Codarea tipului de server în rețele NetWare

Tipul serverului	Cod hexazecimal
Server de fișiere (*File Server*)	4
Poartă de rețea (*Gateway*)	6
Server de imprimantă (*Print Server*)	7
Server-arhivă (*Archive Server*)	9
Server SNA (*System Network Architecture Server*)	21
Punte de comunicație (*Remote Bridge Server*)	24
Poartă TCP/IP (*TCP/IP Gateway*)	27
Server de acces NetWare (*Access Server*)	98

Prin **funcție** se desemnează operațiile efectuate asupra fișierelor (creare, deschidere, redenumire, ștergere, citirea dimensiunii, închidere etc).

NCP folosește IPX pentru transmisia datelor în rețea.

Observații:

1. Spre deosebire de sistemul de adrese IP, în cazul adresării IPX nu există nici o organizație responsabilă cu atribuirea unică a adreselor Novell. Astfel fiecare administrator de rețea este obligat să se asigure că identificatorul de rețea de 32 de biți, exprimat în format hexazecimal, este unic.

2. Adresele de rețea Novell pot fi ierarhizate și alocate în mod unic pe baza adreselor de subrețea IP, prin exprimarea acestora în hexazecimal și adunare cu o unitate. Metoda asigură unicitatea adreselor alocate subrețelelor.

De exemplu, subrețelei cu adresa IP 192.226.26.32 i se asociază adresa IPX C0E21A21.

3. Identificatorul gazdei din adresa Novell coincide cu adresa MAC a plăcii de rețea, ceea ce îi conferă caracterul de unicitate.

4. Este comodă identificarea nodurilor dintr-o rețea Novell (servere, rutere etc) pe baza unor nume (combinații alfa-numerice) asociate adreselor numerice IPX.

5. Operația PING de testare a conexiunilor poate fi aplicată și pe adrese IPX (*PING Extended*).

6. Filtrarea traficului, de includere sau excludere, se poate face și pe baza adreselor Novell, în același mod în care se realizează filtrarea IP.

7. Pentru gestionarea rețelelor Novell se folosesc baze de date cu informații de management (MIB), ca și în cazul rețelelor TCP/IP. Spre deosebire de acestea, unde se aplică protocolul SNMP special creat pentru managementul rețelei, accesarea MIB în rețele Novell se face cu protocolul IPX, prin intermediul unor contoare (*IPX counter*).

8. Rutarea pachetelor între rețele locale NetWare se face pe baza protocolului RIP, care folosește IPX pentru transmisia și actualizarea periodică a informațiilor din tabelele de rutare.

II.3 Suita de protocoale ATM

În modul de transfer asincron (ATM - *Asynchronous Transfer Mode*) datele sunt transmise fragmentat, în **celule** de lungime fixă de 53 de octeți, ceea ce permite transferul datelor la viteze foarte mari.

Tehnologiile ATM permit realizarea comunicațiilor digitale de bandă largă (*broadband*) și de mare viteză (de ordinul GBps), cu aplicații multimedia, transmisii audio și video în timp real.

Primii cinci octeți din celula ATM formează **antetul ATM,** care include un identificator de canal virtual (VCI - *Virtual Channel Identifier*) și suma de control a antetului (HEC - *Header Error Control*) de un octet, calculată pe baza unui polinom ciclic (CRC).

Câmpul datelor din celula ATM are lungime fixă de 48 de octeți.

Comunicațiile ATM se realizează pe baza **modelului ATM,** structurat pe trei nivele (Fig.II.20).

<table>
<tr><th>Nivele OSI</th><th>Nivele ATM</th><th>Subnivele ATM</th></tr>
<tr><td rowspan="2">3/4</td><td rowspan="2">AAL</td><td colspan="2">SSCS</td></tr>
<tr><td>CPCS</td><td>C S
SAR</td></tr>
<tr><td>2/3</td><td>ATM</td><td></td></tr>
<tr><td>2</td><td rowspan="2">Fizic</td><td>TC</td></tr>
<tr><td>1</td><td>PMD</td></tr>
</table>

Fig.II.20 Modelul ATM

Nivelul fizic ATM, echivalent nivelului de acces la rețea din modelul TCP/IP, este împărțit în două subnivele:

1. **subnivelul dependent de mediul fizic** PMD (*Physical Medium Dependent*) - pe acesta sunt definite interfețele fizice spre canalul de comunicații iar transmisia se face serial ca șir de biți;

2. **subnivelul de convergență a transmisiei** TC (*Transmission Convergence*), echivalent cu nivelul "legătură de date" din modelul OSI, realizează conversia celulelor ATM în flux de biți și controlul erorilor pe antetul celulei.

Nivelul ATM, echivalent nivelului de rețea din modelele OSI și TCP/IP, definește structura celulelor, realizează controlul fluxului, gestionează circuitele virtuale de transmisie asemenea subnivelului LLC din modelul OSI.

Nivelul de adaptare ATM (AAL - *ATM Adaptation Layer*) se împarte în două subnivele:

1. **subnivelul comun de convergență** CPCS (*Common Part Convergence Sublayer*) - este independent de serviciile furnizate, fiind responsabil de pregătirea datelor în vederea transmisiei în rețeaua ATM , mai precis stabilirea încărcăturii celulei ATM (*payload*) de 48 de octeți.

2. **subnivelul de convergență a serviciilor** SSCS (*Service Specific Convergence Sublayer*) este dependent de serviciile furnizate utilizatorului (transfer de fișiere, poștă electronică, transmisii video la cerere, de foarte bună calitate etc) și răspunde de siguranța transmisiei datelor.

CPCS include la rândul său alte două subnivele:

1. **subnivelul de convergență** CS (*Convergence Sublayer*) - realizează controlul erorilor prin introducerea la sfârșitul secvenței de date a unui câmp de control de 8 octeți și formatează cadrele de date în vederea segmentării, mai precis completează secvența cu zerouri (*padding*) astfel ca lungimea ei să fie un multiplu de 48 de octeți.

2.**subnivelul de segmentare și reasamblare** SAR (*Segmentation And Reassemble*) fragmentează la emisie unitatea de date în subcelule de 48 de octeți pe care le reasamblează la recepție.

Transmisiile ATM pot fi cu sau fără conexiune, cu viteză de transmisie fixă (CBR - *Constant Bit Rate)* sau variabilă (VBR - *Variable Bit Rate*).

Comunicațiile ATM sunt descrise prin **calitatea serviciului** (QoS - *Quality of Service*).

CBR și VBR sunt definite de Forumul ATM ca fiind clase ale QoS.

CBR se utilizează pe conexiunile care depind de precizia de sincronizare a ceasurilor de transmisie.

În cazul în care rata de transmisie poate varia, QoS definește o altă clasă ABR (*Available Bit Rate*) care are ca obiectiv transmisia integrală a datelor, fără a ține cont de întârzierile de transmisie sau pierderile de celule.

ITU-T (*International Telecommunication Union - Telecommunication Standardisation Sector*) propune utilizarea a patru tipuri de nivele AAL, fiecare cu protocoale specifice:

AAL 1 - pentru transmisii în rețea ATM orientate pe conexiune, cu întârzieri minime de transmisie și CBR (de exemplu, pentru transmisii video isocrone fără compresie).

AAL 2 - pentru transmisii ATM orientate pe conexiune, cu rată variabilă de transmisie (de exemplu, tranmsisii vocale).

AAL 3/4 - pentru transmisii de mare viteză a datelor în rețele ATM comutate, cu sau fără conexiune.

Deși tehnologiile ATM au fost inițial utilizate numai în rețele de arie largă, în prezent se caută soluții de realizare a unor rețele locale pe modelul ATM (ATM LAN), cu servere de emulare (LES - *LAN Emulation Server*) pentru adresarea IP, denumite de IETF (*Internet Engineering Task Force*) servere ATMARP.

Transmisia pachetelor IP în rețele ATM impune conversia de format a unității de date transmise, adică a pachetelor IP în celule ATM la sursă și conversia inversă la destinație. Această operație de conversie a formatului unității de date se numește **emulare**.

Pentru transmisii spre adrese de destinație multiple, se pot utiliza servere de broadcast (BUS - *Broadcast/Unknown Server*) care dispun de conexiuni cu toate calculatoarele din LAN-ul ATM.

În rețelele ATM, rutarea se realizează cu **comutatoare ATM** (*ATM switches*). Acestea aleg **calea de transmisie**, care include mai multe **căi virtuale**, fiecare fiind formată din mai multe **circuite virtuale** (Fig.II.21). Sunt necesari doi identificatori: unul de cale virtuală, VPI (*Virtual Path Identifier*) și unul de circuit virtual, VCI (*Virtual Channel Identifier*).

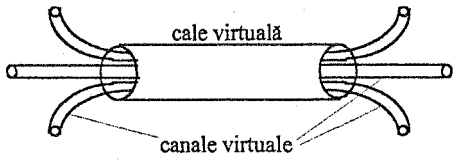


Fig.II.21 Structura de multiplexare ATM

Nivelul ATM este orientat pe conexiune și stabilește formatul celulei transmise, care diferă în funcție de echipamentele între care se face transmisia.

În cazul comunicației client-rețea, se folosește **interfața utilizator-rețea** UNI (*User-Network Interface*) care încapsulează cei 48 de octeți de date cu un antet alcătuit din:

- câmpul general de control a fluxului GFC (*General Flow Control*) (4 biți);
- identificatorul căii virtuale VPI (*Virtual Path Identifier*) de un octet;
- identificatorul canalului virtual VCI (*Virtual Channel Identifier*) de doi octeți;
- un câmp de 3 biți care specifică tipul datelor PTY (*Payload Type*);
- un bit de prioritate CLP (*Cell Loss Priority*);

- câmpul de control a erorilor asupra antetului ATM (1 octet).

Comunicația între două comutatoare ATM se face prin **interfața NNI** (*Network - Network Interface*) care are o structură mai simplă decât UNI, prin cumularea câmpurilor GFC și VPI într-un singur VPI de 12 biți.

Un alt protocol de adaptare, AAL 5, propus inițial propus sub numele de SEAL (*Simple Efficient Adaptation Layer*), reduce dimensiunea câmpului de date din celula ATM la 44 de octeți și mărește lungimea sumei de control la 5 octeți. AAL 5 este superior protocolului AAL 3/4 ca eficiență de transmisie. Totuși AAL 5 nu folosește numere de secvență și nici nu face distincția între celulele care transportă informații utile și cele de control.

Pentru transmisia pachetelor IP prin intermediul rețelelor de transport ATM (*IP over ATM*) se folosește AAL 5 (RFC 1483, RFC 1577).

Rețelele ATM de mare viteză sunt deosebit de atractive pentru transmisii multimedia în timp real, cum sunt transmisiile video la cerere. În acest caz, programul de aplicații video folosește algoritmi de codare/decodare video (MPEG), un protocol de transport și o interfață cu protocolul AAL5 care face trecerea în stiva de protocoale ATM. Cerințele pentru un astfel de sistem sunt deosebite, fiind necesare capacități mari de memorie și procesoare de mare viteză.

III

STANDARDE DE REȚELE LOCALE

III.1 Standarde ETHERNET. Standardul IEEE 802.3

Folosind metoda CSMA/CD de acces la mediu, având o topologie logică de tip *broadcast* și una fizică de tip "magistrală" (*bus*) sau "stea" (*star*), corporațiile Intel, Xerox și Digital au dezvoltat standardele Ethernet I, în 1981, și Ethernet II, în 1982.

Ethernet II este echivalent cu standardul IEEE 802.3 cu mici diferențe în formatul cadrului de date (Fig.III.1).

Preambul 8 octeți	Adresa destinație 6 octeți	Adresa sursă 6 octeți	Tipul protocolului 2 octeți	Câmpul de date 46 - 1500 octeți	Câmp de control a erorilor (FCS) 4 octeți

a. Formatul cadrului ETHERNET II

Preambul 7 octeți	Câmp de START 1 octet	Adresa destinație 6 octeți	Adresa sursă 6 octeți	Câmp de lungime 2 octeți	Câmp de date LLC IEEE 802.2 46 - 1500 octeți	Câmp de control a erorilor (FCS) 4 octeți

b. Formatul cadrului în standard IEEE 802.3

Fig. III.1 Încapsularea datelor în standardele Ethernet și IEEE 802.3

Cadrul de început Ethernet sau preambulul de 8 octeți are rolul de a anunța prezența datelor în rețea și de a asigura sincronizarea plăcii de rețea cu datele recepționate. Similar lucrează cei 8 octeți din preambulul și câmpul de start al cadrului IEEE 802.3.

Adresele sursă și destinație sunt adrese MAC de 6 octeți, stocate în memoria ROM a fiecărei plăci de rețea Ethernet. Primii 3 octeți sunt atribuiți de IEEE (*Institute of Electrical and Electronic Engineers*) pentru identificarea producătorului iar ceilalți 3 octeți sunt stabiliți chiar de către acesta. Astfel adresele MAC sunt unice pe întreg globul.

Tipul protocolului este precizat în cadrul Ethernet prin valori hexazecimale prestabilite de IEEE. De exemplu, 08.00H este atribuit suitei de protocoale TCP/IP iar 81.37H pentru protocolul IPX (*Internetwork Packet eXchange*).

Similar, în cadrul IEEE 802.3 în câmpul de lungime se specifică lungimea câmpului de date.

În câmpul datelor, se intercalează în antet (*header*) codul SAP (*Service Access Point*) de un octet care specifică tipul protocolului folosit la transmisie conform standardului IEEE 802.2 (NetWare 802.2). De exemplu, codul SAP pentru protocol Novell este E0H iar pentru TCP/IP este 06H. Pentru a facilita compatibilitatea tuturor protocoalelor IEEE 802, s-a introdus protocolul SNAP (*SubNetwork Access Protocol*) care impune folosirea unui antet de 5 octeți. Primii trei octeți (DSAP - *Destination SAP;* SSAP - *Source SAP;* Control) alcătuiesc **identificatorul de organizare** iar ultimii doi corespund așa-numitului câmp **EtherType** de 2 octeți, a cărui valoare precizează protocolul folosit. Astfel, TCP/IP corespunde valorii EtherType 08.00H. Identificatorul de organizare complet nul arată că este vorba de un cadru Ethernet.

Detecția erorilor de transmisie din câmpurile precedente (adrese, tip și date) se realizează pe baza unui cod ciclic (CRC - *Cyclic Redundancy Checking*), în câmpul final (FCS - *Frame Check Sequence*).

Standardele Ethernet pot fi aplicate în diverse medii fizice de transmisie rezultând mai multe variante, cu transmisie în banda de bază (BB - *BaseBand*) (Tabel III.1) sau cu modulare și demodulare, cum ar fi 10 Broad 36 la 10 Mbps, pe segmente de rețea de maximum 3600 metri.

Observație

Limitarea impusă lungimii maxime a unui **segment** de rețea (porțiunea de cablu cuprinsă între două componente sau noduri adiacente) este determinată de fenomenul de atenuare specific mediului fizic de transmisie și încărcării capacitive produse de linie. În standardul 802.3, cablul coaxial utilizat are impedanța lineică de 50 ohmi.

Standardul 10 Base-T este practic cel mai utilizat datorită avantajelor sale evidente: protocol de comunicație simplu; stațiile pot fi conectate la rețea în timpul funcționării acesteia; se utilizează cabluri pasive, fără modemuri; nu se folosește jeton de transmisie.

Arhitectura 10 Base-T admite un diametru al rețelei de 2500 m și maximum 4 repetoare sau hub-uri între oricare două noduri terminale din rețea. Lucrând pe principiul CSMA/CD, rețeaua admite apariția coliziunilor între pachete cu înștiințarea stațiilor ale căror pachete nu au fost transmise la destinație pentru a se proceda la retransmisia lor. Fiecare stație așteaptă această posibilă notificare de coliziune pe un interval de timp corespunzător la maxim 512 biți transmiși.

Tabel III.1

Standarde Ethernet cu transmisie în banda de bază

Standard	Viteză de transmisie (Mbps)	Mediu de transmisie	Lungime maximă a segmentului (m)	Număr maxim de noduri și segmente
1Base5 (StarLAN)	1	Cablu simetric torsadat neecranat (UTP - *Unshielded Twisted Pair*) Conector RJ45	500	100
10Base2	10	Cablu coaxial subțire (RG - 8) Conector BNC	185	30
10Base5 (StarLAN10)	10	Cablu coaxial gros (RG - 58) Conector BNC	500	100
10BaseT	10	Cablu UTP Conector RJ45	100	1024
10BaseF	10	Cablu de fibră optică multimod	1000	1024

În 1995, pentru creșterea vitezei de transmisie folosind aceleași medii fizice, a apărut standardul "Ethernet rapid" (*Fast Ethernet*), echivalent cu IEEE 802.3u, notație mai puțin folosită. Acesta are la bază coduri de linie binare sau ternare (tehnici ADSL - *Asymmetrical Digital Subscriber Line*), aplicate la viteze de clock mai mari, care modelează spectrul de frecvențe al datelor și facilitează sincronizarea sistemului, astfel încât rata de transmisie crește la 100 Mbps cu menținerea lungimii maxime a segmentelor de cablu (Tabel III.2).

Standardul 100BaseTX sau 100BaseT aplică pe subnivelul MAC standardul IEEE 802.3 dar transmite de 10 ori mai rapid decât 10BaseT ceea ce determină o reducere a diametrului maxim al rețelei la 210 m. În general, plăcile de rețea 100BaseT sunt notate 10/100 Ethernet, adică pot fi utilizate la ambele valori ale vitezei de transmisie dar nu simultan. Există și echipamente de comunicații care pot lucra și la 10 Mbps, și la 100Mbps (punți, comutatoare, routere). Există

hub-uri la care pot fi conectați utilizatori dintr-o subrețea 100BaseT cu alții care lucrează în rețea 10BaseT însă apar probleme legate de eventualele erori de depășire a capacității de memorie urmate de pierderea datelor.

Tabel III.2

Standarde Fast Ethernet de 100 Mbps

Standard	Mediu de transmisie	Lungime maximă a segmentului (m)	Cod de linie	Observație
100Base-T4	CAT 3; 4; 5 UTP (8 fire)	100	Manchester (BIF-L)	Semnalizări la 25 MHz.
100Base-TX	CAT 5 UTP (4 fire) CAT 1 STP (*Shielded Twisted Pair*) (4 fire)	100	4B5B (125 Mhz)	Transmisie full duplex la 100 Mbps; half-duplex la 200 Mbps.
100Base-FX	Cablu de fibră optică multimod (2 fire)	2000	RZ	Full duplex la 100Mbps la mare distanță

Evitarea coliziunilor dintr-o rețea Ethernet 100BaseT și a întârzierilor de transmisie specifice rețelelor IBM Token-Ring, se realizează în rețelele **100BaseVG** (IEEE 802.12) echivalente cu 100BaseTX, prin modificarea metodei de acces la mediu. În loc de CSMA/CD se aplică metoda de acces la mediu la cerere, pe bază de priorități (DPMA - *Demand Priority Media Access*), prin protocolul DPP (*Demand Priority Protocol*). Accesarea se face prin apelarea succesivă a stațiilor de către hub (schema *round-robin polling),* cu posibilitatea modificării dinamice a valorilor de prioritate pentru a se evita monopolizarea rețelei de către un număr redus de terminale. Într-o rețea 100BaseVG, se pot transmite cadre în standarde diferite (802.3 sau 802.5), dar nu simultan în aceeași rețea. Pentru interconectarea a două rețele în standarde diferite sunt necesare echipamente de comunicație (routere VG) care să realizeze conversia cadrelor dintr-un standard în celălalt. Arhitectura 100BaseVG este utilă în aplicații multimedia.

Pentru creșterea numărului de utilizatori dintr-un LAN 802.3 și a vitezei de transmisie, se poate realiza **o rețea 802.3 comutată** folosind un comutator (*switch*) cu un modul de bază (*backplane*) de mare viteză (>1Gbps), care interconectează 8, 16 sau mai multe plăci de rețea, de obicei cu conexiuni 10BaseT.

În prezent, se utilizează și standardul **Gigabit Ethernet** sau **GigaEthernet**, echivalent cu IEEE 802.3z, pentru LAN cu topologie fizică 'star', logică 'bus', 1000 MBps, în variantele:

1. 1000 Base CX - LAN în cablu coaxial dual de maxim 25 de metri.
2. 1000 Base T - LAN cu CAT 5 UTP, segment de 100m.

3. 1000 Base SX - LAN, pe fibră optică multimod (830 nm), segmente de cablu de 550m.

4. 1000 Base LX - LAN fie pe fibră optică multimod, pe segmente de cel mult 550 metri lungime, fie pe fibră optică unimod cu lungime a segmentelor de până la 5 km. Transmisia se face pe lungimea de undă de 1270 nm.

III.2 Standardul IEEE 802.4. Rețea Token-Bus

Dezavantajul major al standardului 802.3 este acela că, neavând stabilite priorități, există riscul ca o stație să aștepte la infinit eliberarea liniei și să nu poată transmite date, deci cazul cel mai defavorabil este nelimitat în timp. Acest fapt este nepermis pentru aplicațiile în timp real și pentru procesele de automatizare.

S-a propus atunci folosirea unei topologii logice de tip 'inel' care limitează durata maximă a intervalului în care o stație nu poate transmite. Nu s-a adoptat topologia fizică de 'inel' deoarece există riscul blocării rețelei prin întreruperea cablului de transmisie.

Standardul IEEE 802.4 (1985), descrie un LAN cu topologie fizică "liniară" (*bus*) sau "arbore" (*tree*), topologie logică "în inel" (*logical ring*) și acces la mediu cu cerere pentru acordarea permisiunii de transmisie (metoda *Token Passing*), rețeaua fiind denumită **"token-bus"** adică LAN cu jeton pe magistrală (Fig.III.2). Ordinea numerotării stațiilor este aleatoare, acestea fiind conectate la magistrala de date (*data bus*) în rețea cu difuzare. În general, se utilizează cablu coaxial de 75 ohmi, datele fiind modulate CPFSK (*Continuous Phase Frequency Shift Keying*) sau PSK (*Phase Shift Keying*) coerent, precodat duobinar. Datele pot fi transmise la viteze de 1, 5 sau 10 Mbps.

În cazul particular prezentat în figura III.2, stația 6 nu este inclusă în inelul logic în momentul în care intră în funcțiune rețeaua.

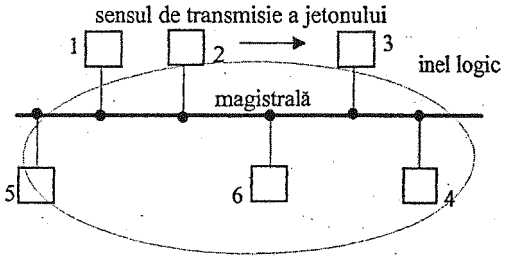


Fig.III.2 Rețea Token-bus

Protocolul MAC prevede posibilitatea includerii și excluderii stațiilor din inelul logic, prin procedeul de "învățare" (*learning*) bazat pe citirea adreselor sursă și destinație din antetele mesajelor transmise.

În fapt, inelul logic constă într-o listă de adrese pe baza cărora se acordă stațiilor permisiunea de transmisie, marcată de cadrul special denumit **jeton** (*token*).

Standardul IEEE 802.4 este mai complicat și totodată incompatibil la nivel fizic cu IEEE 802.3.

Formatul cadrului în standard 802.4 este prezentat în figura III.3, cu specificarea lungimii câmpurilor componente în octeți (B - *Bytes*).

Preambul	Câmp de start	Câmp de control	Adresa destinație	Adresa sursă	Câmp de date	Sumă de control	Câmp de delimitare
≥ 1octet	1 octet	1 octet	2 sau 6 B	2 sau 6B	0 - 8182B	4 octeți	1 octet

Fig. III.3 Cadrul IEEE 802.4

Câmpul de control diferențiază cadrele de date de cele de control. În **cadrele de date**, acesta conține fie prioritatea cadrului cu valori de 0 (prioritate minimă), 2, 4 sau 6 (prioritate maximă), fie indicatorul privind recepția corectă sau incorectă a datelor. În **cadrele de control**, acest câmp specifică tipul cadrului (Tabel III.3). Spre deosebire de IEEE 802.4, în standardul IEEE 802.3 nu există cadre de control.

Observație

Nu este exclusă varianta jetoanelor multiple. Pentru evitarea coliziunilor, dacă o stație sesizează că și altă stație deține jetonul, atunci renunță la propriul jeton. Dacă, accidental, nu mai există nici un jeton, se va reinițializa inelul logic (vezi Anexa A). Acest principiu de soluționare a coliziunilor se aplică și în sistemele *wireless,* cu transmisie radio.

Avantajele acestui standard constau în:

- utilizarea cablurilor de înaltă fiabilitate;
- dispune de un sistem de priorități;
- garantează utilizarea fracțiunii alocate de bandă pentru prioritățile mari (de exemplu, voce digitizată);
- poate suporta mai multe canale pe cabluri de bandă largă cu transmisie TDM (*Time Division Multiplexing*).

Tabel III.3

Câmpul de control din cadrul de control IEEE 802.4

Valoarea înscrisă în câmpul de control	Procedura efectuată	
	Denumire	Semnificație
00H	*Claim_token*	Se cere jetonul pentru inițializarea inelului logic.
01H	*Solicit_succesor_1*	Deținătorul jetonului permite altor stații să intre în inel.
02H	*Solicit_succesor_2*	Dacă nu se identifică primul succesor, deținătorul jetonului rulează protocolul standard de tratare a conflictelor pentru a reface inelul.
03H	*Who_follows*	Dacă succesorul nu este activ, se caută un nou succesor, pentru a elimina stația căzută din inel
04H	*Resolve_contention*	Deținătorul jetonului rulează un algoritm de arbitrare în cazul unui conflict în rețea.
08H	*Token*	Se transmite jetonul stației cu adresa specificată în cadru.
0AH	*Set_succesor*	În momentul ieșirii din inel, o stație C cu predecesorul P și succesorul S, transmite lui P adresa noului său succesor, S.

Totuși acest standard complex are **și o serie de dezavantaje:**

- nu poate fi implementat pe fibră optică;
- necesită modemuri și amplificatoare de bandă largă;
- întârzierile de transmisie pot fi relativ mari.

III.3 Standardul IEEE 802.5. Rețea Token-Ring

Spre deosebire de IEEE 802.3, standardul IEEE 802.5, adoptat în 1985, nu specifică viteza de transmisie a datelor. Având o topologie logică secvențială ("în inel"), una fizică tradițională de tip "inel" (*ring*), dar mai folosită fiind cea de tip "stea" (*star*), cu acces la mediu prin metoda jetonului (*token passing*), arhitectura de rețea propusă de IBM și denumită **Token-Ring** poate lucra la viteze de 1, 4 sau 16 Mbps, pe cablu simetric torsadat (Fig.III.4), cu formatul cadrului transmis stabilit de standardul IEEE 802.5 (Fig.III.5).

Pentru a se evita situațiile de întrerupere a inelului și de blocare totală a rețelei, toate stațiile pot fi conectate prin relee, la un **centru de cablare** (*wiring center*), în topologie fizică de tip 'stea', rezultând un **inel cu configurație de stea** (*star-shaped ring* sau *star-ring*).

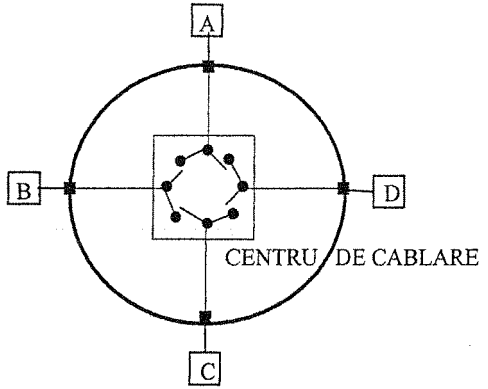


Fig. III.4 Rețea Token-Ring cu centru de cablare

Supravegherea funcționării inelului fizic se face printr-o **stație de monitorizare** (*monitor station*) care de fapt, poate fi oricare stație din rețea.

SD	AC	FC	Adresa destinației	Adresa sursei	Câmp de date	Sumă de control	ED
1B	1B	1B	6 B	6B	(nelimitat)	4B	1B

Fig. III.5 Cadrul IEEE 802.5

Semnificațiile notațiilor folosite în cadrul IEEE 802.5 sunt următoarele:

SD - *Starting Delimiter*	Delimitator de început de cadru
AC - *Access Control*	Controlul accesului
FC - *Frame Control*	Specifică tipul cadrului (de date sau de control)
ED - *Ending Delimiter*	Delimitator de sfârșit de cadru
FS - *Frame Status*	Octet de stare a cadrului, specificată prin biții A și C:
	A=0; C=0: destinația nu este găsită;
	A=1; C=0: destinația există, dar nu acceptă cadrul;
	A=1; C=1: destinația există și copie cadrul.

Jetonul este un cadru format din trei octeți: SD, AC și ED. Jetonul circulă permanent în rețea până ce este preluat de una din stații care va transmite cadre de date. Durata maximă alocată pentru transmisia și păstrarea jetonului (*token-holding time*) este tipic de 10 msec, ceea ce corespunde unei lungimi de cadru de 5000 de octeți, la viteza de transmisie de 4 Mbps.

Octetul AC conține un câmp care precizează prioritatea jetonului. Pentru transmisia unui cadru cu gradul de prioritate *n* se așteaptă apariția unui jeton de prioritate mai mică sau egală cu *n*.

Jetonul poate fi rezervat pentru următoarea transmisie de stațiile cu prioritate egală sau mai mare decât *n*. Se observă posibilitatea creșterii nelimitate a priorității ceea ce ar conduce la netransmisia cadrelor de prioritate inferioară. De aceea, stația care crește prioritatea jetonului la un anumit moment, este obligată să o scadă după ce termină transmisia.

Cadrul de control 802.5 conține un **câmp de control** care specifică procedura ce trebuie efectuată (Tabel III.4).

Tabel III.4

Câmpul de control în cadrul de control IEEE 802.5

Valoarea înscrisă în câmpul de control	Procedura efectuată	
	Denumire	Semnificație
00H	*Duplicate Address Test*	Testează adresele stațiilor pentru a sesiza posibila lor coincidență.
02H	*Beacon* (Baliză)	Localizează întreruperile din inel.
03H	*Claim_token*	Stația cere jetonul pentru a deveni 'monitor'.
04H	*Purge*	Elimină cadrele care se propagă la infinit.
05H	*Active monitor present*	Cadru emis periodic de stația 'monitor'.
06H	*Standby monitor present*	Cadru emis de o stație care poate deveni stație 'monitor'.

O chestiune specifică rețelelor 'în inel' o constituie **lungimea fizică minimă a inelului** (L_{min}) care se determină ca produsul dintre **viteza de propagare** (v) specifică mediului (circa 59% din viteza luminii **c** pentru cablu cu conductor metalic, până la 98% din **c** pe fibră optică multi- mod, cu miez de sticlă) și **durata jetonului** (t) de 3 octeți, dedusă în funcție de rata de transmisie a datelor.

Exemplu: Într-o rețea **Token-Ring** implementată cu cablu UTP, la viteza de 1 Mbps:

$L_{\min} = t \cdot v = 24 \cdot \frac{1}{10^6} \cdot 0,59 \cdot 3 \cdot 10^8 = 4248\,m$

Prin conexiunile PP, standardul 802.5 utilizează tehnologii simple, digitale și orice mediu de transmisie. Prin utilizarea centrelor de cablaj, se detectează și se elimină automat blocajele cauzate de defecțiunile de cablu. Dezavantajul major este dat de costul ridicat al plăcilor de rețea utilizate pentru acest standard.

Alegerea unui anumit standard 802 pentru o rețea locală depinde de mai mulți factori: performanțe, costuri și condiții locale privind instalarea.

Interconectarea rețelelor locale cu standarde 802 diferite, incompatibile, constituie o problemă rezolvată prin utilizarea așa-numitelor **punți transparente** (*promiscuous bridge*) denumite și **punți cu arbore de acoperire** adiacent tuturor LAN-urilor sau a **punților cu dirijare de la sursă** (*source routing*).

Incompatibilitatea standardelor IEEE 802.x derivă printre altele din lungimea diferită a cadrelor, din existența sau nu a gradelor de priorități precum și din modul de numerotare a biților dintr-un octet. În standardul IEEE 802.3, cel mai semnificativ bit (MSB - *Most Significant Bit*) al octetului este primul bit din stânga, în timp ce în standardul 802.5 este primul din dreapta. Translarea cadrelor dintr-un standard în altul va impune inversarea ordinii biților din fiecare octet (*Bit-Order Reversal*).

Pentru a transmite pachete între LAN-uri de tip 802.x, puntea va realiza mai multe operațiuni de modificare a formatului cadrelor (Tabel III.5).

Tabel III.5

Operații necesare pentru interconectarea a două LAN-uri

în standarde 802.n (n=3; 4; 5)

		LAN destinație		
		802.3 (CSMA/CD)	802.4 (Token-Bus)	802.5 (Token-Ring)
LAN sursă	802.3	-	b; f; g.	b; c; f; g; i;
	802.4	a; b; c; e; g; j.	j	a; b; c; g; i; j; p.
	802.5	a; b; d; e; g; i; s.	b; d; g; i; p; s.	d; s.

Notații:

a - alertarea destinației de apariția unui cadru prea lung;

b - recalcularea sumei de control (*checksum*);

c - soluționarea congestiilor;

d - drenarea inelului, prin eliminarea cadrelor neexpediate în timp util;

e - eliminarea priorității;

f - generarea priorității fictive;

g - reformatarea cadrului;

i - inversarea ordinii biților;

j - transferarea jetonului;

p - copierea priorității;

s - setarea biților A și C din octetul de stare.

III.4 FDDI

Arhitectura de rețea FDDI (*Fiber Distributed Data Interface*) a fost standardizată de ANSI (*American National Standards Institute*) în 1984 (ISO 9314).

Metoda de acces la mediu este cea cu jeton modificată (*modified token-passing*), topologia logică este secvențială iar fizic rețeaua constă din două inele separate cu sensuri inverse de transmisie (Fig. III.6). Aceasta este de fapt o rețea Token-Ring implementată cu fibră optică multimod (MMF - *MultiMode Fiber*), lucrând la viteza de 100 Mbps, pe distanțe de cel mult 200 km, cu maximum 500 de stații și segmente de cablu de maximum 2 km lungime.

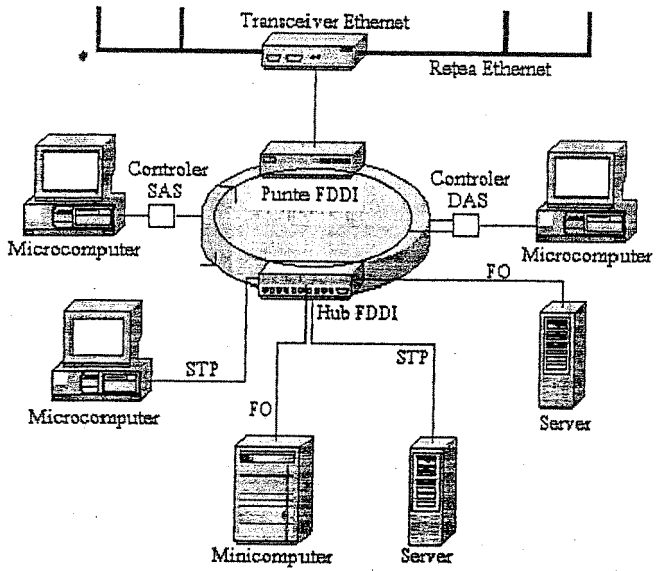


Fig. III.6 Rețea FDDI

Redundanța inelului dual permite continuarea funcționării rețelei chiar dacă unul din inele se întrerupe temporar. Dacă accidental ambele inele se întrerup în același loc, prin interconectarea lor se poate forma un inel unic cu lungimea dublă față de cea a inelelor inițiale.

Un terminal de date poate fi conectat la un singur inel (SAS - *Single-Attachement Station*) sau la ambele inele (DAS - *Dual-Attachement Station*).

Cadrele de date uzuale, având formatul asemănător cu cel din standardul 802.5, se transmit la cerere, în mod asincron.

FDDI permite transmisia unor cadre speciale sincrone în sistem SDH (*Synchronous Digital Hierarchy*). La fiecare 125 μsec se transmite un cadru sincron care conține până la 96 de canale primare de 64 kbps, adică include fie patru canale T1 (24 de căi primare) de 1,544 Mbps, fie trei canale E1 (32 de căi) de 2,048 Mbps.

Astfel, 16 cadre sincrone transmise la fiecare 125 μsec vor include 1536 canale PCM și vor utiliza 98,304 Mbps din cei 100 Mbps disponibili în rețeaua FDDI. În general, restul de bandă neutilizată pentru transmisii sincrone se alocă la cerere, pe baza unui sistem de priorități, pentru transmisiile asincrone.

Rețeaua este imună la interferențe electromagnetice (EMI- *ElectroMagnetic Interference*) și radio (RFI - *Radio Frequency Interference*), fiind mai sigure comparativ cu rețelele radio sau cele cu conductor metalic.

Un LAN FDDI poate fi interconectat ușor cu o rețea Ethernet printr-o punte specială. De asemenea, prin FDDI se pot transmite cadre ISDN (*Integrated Services Digital Network*) de date și voce, standardizate de CCITT (*International Consultative Committee for Telegraphy and Telephony*).

Lățimea de bandă mare, stabilitatea și redundanța oferite de rețeaua FDDI sunt avantaje incontestabile astfel încât aceasta poate fi utilizată ca o 'coloană vertebrală' (*backbone*) de interconectare a mai multor LAN-uri (Ethernet, Token-Bus sau Token-Ring). De asemenea, folosind concentratoare (*hub*-uri) FDDI, se pot grupa mai multe calculatoare (maxim 20) care să dispună fiecare de o lărgime de bandă mult mai mare decât în rețelele cu conductor metalic. O altă variantă de utilizare a arhitecturii și tehnologiei FDDI ar fi interconectarea rețelelor Ethernet cu servere și terminale care necesită lățimi mai mari de bandă (aplicații multimedia, transmisii în timp real etc).

Echipamentele pentru FDDI au costuri relativ mari astfel că în unele aplicații, care necesită viteze de 100 Mbps, se preferă utilizarea rețelelor Ethernet rapide.

Rețelele FDDI sunt mult prea complicate, cu multe echipamente de comunicații (repetoare, concentratoare, punți, routere) iar administrarea lor este dificilă.

Reducerea costurilor este posibilă prin utilizarea în locul fibrelor optice a conductoarelor din cupru ceea ce determină reducerea lungimii maxime admise a segmentelor de rețea de la 2 km la 100 m, la viteze de 100 Mbps. Se obține așa-numita interfață de date CDDI (*Copper Distributed Data Interface*) care respectă standardele ANSI referitoare la FDDI, cu excepția mediului fizic de transmisie și a limitărilor impuse de acesta.

Este dificil de declarat care este cea mai bună arhitectură de rețea pentru o anumită aplicație. Doar printr-o analiză pe baza modelului sus-jos (*top-down*) se poate decide care este arhitectura optimă de rețea într-un caz specific.

III.5 ISO-ETHERNET

Pentru aplicații care trebuie să ruleze în timp real (voce, video, multimedia), o alternativă la 100BaseVG o constituie arhitectura de rețea **Iso-Ethernet** (*Isochronous Ethernet Integrated Services*), descrisă în standardul IEEE 802.9.

Deși nu lucrează la viteze la fel de mari (100 Mbps) ca 100BaseVG, Iso-Ethernet are avantajul că, similar cu standardele ISDN (*Integrated Services Digital Network*) definite pentru rețele de arie largă (WAN), acesta oferă într-o bandă de 16,144 Mbps, o combinație dinamică de servicii specifice:

- un **canal P ISDN** de 10 Mbps pentru trafic Ethernet, compatibil cu 10BaseT.

- un **canal C ISDN** de 6,144 Mbps pentru aplicații în timp real, divizat în maximum 96 de **canale B ISDN** de 64 kbps pentru transmisii multimedia și eventual un **canal D ISDN** de 16 kbps utilizat pentru semnalizări, controlul comutării, transfer de pachete la viteze mici.

Canalul C utilizează același semnal de tact de 8 kHz ca cel folosit în aplicațiile ISDN comerciale în rețelele de arie largă, pentru transmisii la mare distanță. De aici, provine și termenul de **Isochronous** (**Iso** = același; **chronous** = clock).

Într-o rețea Iso-Ethernet, se utilizează pentru interconectarea echipamentelor câte două perechi de cabluri torsadate ecranate (Cat 3/5 STP).

Rețelele Iso-Ethernet au trei moduri specifice de operare:

1. Modul **10BaseT** utilizează doar canalul P pentru conexiuni Ethernet.

2. Modul de **servicii multiple** folosește canalele P și C pentru transmisii video și multimedia.

3. Modul **isocron** împarte banda de 16,144 Mbps în 248 de canale PCM primare de 64 kbps pe care se transmite în timp real semnal vocal sau video.

Includerea rețelei Iso-Ethernet într-o rețea ISDN se face prin intermediul unui hub specializat denumit **unitate de atașare** (AU - *Attachment Unit*) prevăzut cu un port (interfață) de conectare la WAN-ul ISDN.

Un terminal prevăzut cu o placă de rețea (NIC) pentru Iso-Ethernet se numește **echipament terminal cu servicii integrate** (ISTE - *Integrated Services Terminal Equipment*).

Nu toate plăcile de rețea și hub-urile Ethernet trebuie înlocuite pentru trafic isocron, numai cele ale terminalelor care necesită transmisii speciale în timp real (voce, video, multimedia). Orice AU este prevăzută și cu porturi Ethernet pentru conexiuni clasice 10 Base T.

Distanța între interfața WAN și orice terminal din rețeaua locală Iso-Ethernet este de maximum 100 metri.

III.6 STANDARDUL IEEE 802.11. REȚEA WLAN

Transmisia prin undă radio, în spațiu liber, fără fir, este avantajoasă în multe situații în care nu este instalată o rețea de comunicații 'cu fir' sau când între utilizatori distanțele sunt mari și/sau relieful este accidentat. De asemenea, necesitatea asigurării comunicațiilor mobile la nivelul diverselor vehicule (autovehicule, avioane, vapoare) aflate în mișcare, a impus dezvoltarea unui standard pentru rețelele de comunicații 'fără fir' (*wireless*).

Rețelele locale fără fir (WLAN - *Wireless Local Area Network*) sunt descrise în standardul IEEE 802.11.

Transmisia informației digitizate se face prin spațiul liber, prin așa-numitul mediu fizic 'fără fir' (WM - *Wireless Medium*), prin intermediul echipamentelor radio de emisie/recepție și a radioreleelor digitale, precum și a unor echipamente de comunicații specializate (modemuri și routere pentru transmisii radio).

WM este un canal de comunicații cu acces multiplu, pentru care modul de acces la mediu se bazează pe metoda CSMA/CA pentru evitarea coliziunilor. Spre deosebire de metoda CSMA/CD care prevedea testarea mediului fizic înaintea transmisiei, în comunicațiile fără fir este posibil ca o stație să nu detecteze transmisia efectuată de o altă stație din rețea și nici apariția unei coliziuni.

Se aplică două procedee pentru determinarea stării de "liber" sau "ocupat" a mediului de transmisie:

1. **Detecția fizică de purtătoare** (semnal purtător modulat sau nemodulat; semnale de control: RTS - *Request to Send*, CTS - *Clear to Send*). Detecția de semnal se efectuează la nivelul fizic al fiecărui echipament terminal din rețea.

2. **Detecția virtuală a purtătoarei** bazată pe un algoritm de predicție a traficului în rețea, rulat pentru generarea **vectorului de alocare a rețelei** (NAV - *Net Allocation Vector*).

Mediul se consideră "liber" dacă nu se detectează nici un semnal și NAV = 0.

Pentru evitarea pierderii informațiilor în cazul apariției unor coliziuni nedepistate, este necesară confirmarea recepției corecte a cadrelor de către stația de destinație (ACK - *Acknowledge*).

Transmisia efectivă a datelor este precedată de operații de testare a mediului, sincronizare și autentificare.

Standardul **IEEE 802.11** prevede ca transmisia la distanță să se efectueze fie prin undă **radio**, cu extensie de spectru cu salturi de frecvență (FHSS - *Frequency Hopping Spread Spectrum*) sau cu secvență directă (DSSS - *Direct Sequence Spread Spectrum*), fie în **infraroșu** (IR - *InfraRed*), la viteze de transmisie de ordinul 1, 2, 3 Mbps în banda de 2,4 GHz.

Varianta **IEEE 802.11a** descrie rețelele locale de comunicație cu transmisie radio în banda de 5 GHz, la viteze cuprinse între 6 și 54 Mbps, folosind tehnica OFDM (*Orthogonal Frequency Duplexing Method*).

Varianta **IEEE 802.11b** se referă la rețelele de comunicații digitale 'fără fir',cu transmisie în banda de 2,4 GHz, cu viteze de 5,5 Mbps (duplex) și 11 Mbps (semi-duplex), cu salturi de frecvență (FHSS).

Rețelele de comunicație 'fără fir' pot fi interconectate cu cele cu transmisie pe cablu.

În general, stațiile de lucru sunt grupate în **celule**, delimitate spațial sau geografic, în funcție de aria de acoperire (BSA - *Basic Service Area*) a echipamentelor radio de emisie/recepție (Fig. III.7). Totalitatea terminalelor dintr-o celulă reprezintă **setul de bază** (BSS - *Basic Service Set*).

Fiecare stație sau rețea locală fixă inclusă într-o celulă WLAN trebuie să dispună de un **adaptor** (STA - *Station Adapter*) care să realizeze comunicația radio.

Accesul din exterior la o celulă se face la nivelul **punctului de acces** (AP - *Access Point*), adică al hub-ului radio (*wireless*).

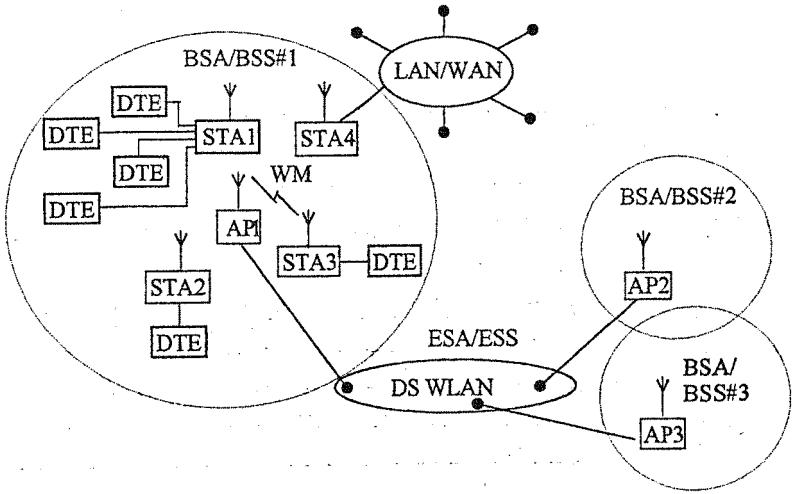


Fig.III.7 Arhitectură WLAN

Există posibilitatea formării unei rețele WLAN ad-hoc, fără AP, cu echipamente portabile care alcătuiesc un set independent de stații (IBSS - *Independent BSS*). Comunicațiile între celulele aceluiași sistem se realizează prin intermediul **sistemului de distribuție** (DS - *Distribution System*).

Celulele pot fi fie disjuncte, fie suprapuse parțial sau total. Pentru un sistem cu mai multe celule se definește aria extinsă de acoperire (ESA - *Extended Service Area*), care include setul extins de stații terminale (ESS - *Extended Service Set*).

O modalitate aparte de comunicații de date 'fără fir' este oferită de sistemele de telefonie mobilă, cu separarea celulelor adiacente în frecvență, ceea ce elimină problemele generate de interferențe nedorite și coliziuni.

Toate sistemele de comunicații prin undă radio, indiferent de aplicație (transmisii de date, voce, semnal audio-video), sunt afectate de fenomenul de fading cauzat de propagarea semnalului pe căi multiple și interferențele dintre semnalul util și replicile reflectate de obstacole fixe sau mobile ale acestuia, fiind necesară utilizarea unor tehnici de codare performante pentru detecția și corecția erorilor de transmisie.

III.7 ANALIZA STANDARDELOR LAN PE BAZA MODELULUI OSI

În figura III.8, se observă pe ce nivele ale modelului OSI lucrează câteva din standardele elaborate pentru rețelele locale de calculatoare, precum și unele protocoale din suitele TCP/IP și IPX/SPX. Nivelele OSI superioare sunt implementate software.

<table>
<tr><td>4</td><td colspan="2">NIVEL TRANSPORT</td><td colspan="7">TCP, SPX</td></tr>
<tr><td>3</td><td colspan="2">NIVEL REȚEA</td><td colspan="7">IP, IPX</td></tr>
<tr><td rowspan="2">2</td><td rowspan="2">LEGĂTURĂ DE DATE</td><td>LLC</td><td colspan="7">IEEE 802.2</td></tr>
<tr><td>MAC</td><td>IEEE 802.3
ETHERNET
FAST ETHERNET</td><td>IEEE 802.4
TOKEN BUS</td><td>IEEE 802.5
TOKEN RING</td><td>IEEE 802.9
ISO ETHERNET</td><td>IEEE 802.11
WLAN</td><td>IEEE 802.12
100 BASE VG</td><td>ISO 9314
FDDI</td></tr>
<tr><td>1</td><td colspan="2">NIVEL FIZIC</td><td colspan="7"></td></tr>
</table>

Fig. III.8 Standarde și protocoale de comunicații pentru LAN

IV

ECHIPAMENTE DE COMUNICAȚII PENTRU LAN

IV.1 CABLURI DE TRANSMISIE

EIA (*Electronics Industries Association*) și TIA (*Telecommunication Industry Association*) au elaborat în comun o serie de standarde, cunoscute ca standarde TIA/EIA, referitoare la proiectarea și instalarea rețelelor de calculatoare. Se iau în considerare elemente specifice acestora:

- cablarea orizontală;
- dulapurile (*rack*) pentru echipamentele de telecomunicații;
- cablarea magistralelor;
- camerele de echipamente;
- ariile de lucru;
- facilitățile de intrare.

Cablarea orizontală (*horizontal cross-connect*) incluzând mediul fizic de comunicație locală, dintre stațiile de lucru, echipamentele de comunicație (hub, switch) și dulapurile cu echipamente, este descrisă de **standardul TIA/EIA-568-A.**

Acest standard specifică tipurile și performanțele cablurilor de comunicații și impune existența a minimum două ieșiri în prize pentru fiecare zonă de lucru, dintre care un cablu UTP (*Unshielded Twisted Pair*) iar al doilea poate fi de orice tip. Este permisă realizarea punctelor de tranziție (*Transition Point*), adică joncțiunile dintre segmentele de cablu de același tip.

UTP este un cablu torsadat în pereche, neecranat, conținând 4 perechi de fire.

Prin **fir** se denumește conductorul metalic izolat electric.

Fiecare pereche de fire este răsucită, cu un pas de torsadare cuprins între 80 și 200 mm, care diferă de la o pereche la alta. În plus, perechile sunt torsadate între ele, cu un pas de 300 mm, pentru reducerea diafoniei dintre ele (*crosstalk*).

Perechile sunt învelite într-o manta de protecție mecanică, realizată din material plastic.

Impedanța caracteristică a perechii de cablu UTP are valoarea tipică de 100 Ohmi.

Diamentrul exterior al cablului este de 0,43 cm, dimensiunile sale mici și prețul redus constituind avantaje în alegerea acestui cablu pentru rețelele de calculatoare.

Mufarea cablului pentru conexiuni într-o rețea de calculatoare se face cu un clește de sertizare (*crimper*), cu conectori RJ-45 (*Registered Jack -45*), modular cu 8 pini, cu transmisie serială asincronă, pentru rețele 10 Base T. În alte cazuri se folosește fie conectorul RJ-11 telefonic cu 4 căi pentru transmisii telefonice, fie RJ-12, cu 6 căi pentru transmisii vocale în rețea ISDN.

Izolațiile firelor sunt de culori diferite (codul culorilor), pentru a permite identificarea perechilor de fire și corespondența lor la capetele cablului.

Necesită folosirea repetoarelor de semnal pentru lungimi mai mari de 100 m, care să compenseze atenuarea proprie a cablului.

Cablul UTP nu este protejat față de interferențele electromagnetice și radio externe. Se preferă instalarea separată (nu în același canal de cablu) față de alte cabluri (telefonice sau de alimentare cu energie electrică).

Se utilizează în rețelele Ethernet (10 Base T), Fast Ethernet (100 Base T) și GigaEthernet (1000 Base T).

Sunt definite 5 categorii de cablu UTP (CAT1, CAT2, CAT3, CAT4, CAT5). Pentru LAN se pot utiliza, în funcție de frecvența maximă de lucru, UTP CAT3 (< 16 MHz), CAT4 (< 20 MHz) și CAT5 (< 100MHz), cea din urmă fiind cea mai utilizată în prezent. Ultimele standarde prevăd și categoriile CAT5e (< 100 MHz), CAT6 (< 250MHz) și CAT7 (< 600MHz).

STP (*Shielded Twisted Pair*) este un cablu torsadat în pereche, ecranat, conținând 4 perechi de fire. Fiecare pereche de fire este torsadată și ecranată cu o folie metalică (*pair shield*).

Toate perechile sunt ecranate electromagnetic cu un ecran suplimentar de grup (*overall shield*) de tip folie sau panglică metalică. La exterior, se folosește o manta din material plastic, pentru protecție împotriva factorilor mecanici sau de climă.

Acest cablu permite minimizarea efectelor diafoniei dintre perechi și a interferențelor electromagnetice (EMI - *ElectroMagnetic Interference*) sau radio (RFI - *Radio Frequency Interference*) din exteriorul cablului și a radiațiilor proprii spre exterior.

Impedanța caracteristică a perechii din cablul STP are valoarea tipică de 150 Ohmi.

Dezavantajele STP constau în dimensiune, greutate și preț mai mari comparativ cu UTP.

Mufarea cablului se face cu un clește de sertizare, cu conectori STP, cunoscând codul culorilor.

Asemenea UTP, necesită folosirea repetoarelor de semnal pentru lungimi mai mari de 100m și sunt definite ami multe categorii de cablu.

ScTP (*Screened Twisted Pair*) este un cablu torsadat în pereche, izolat, conținând 4 perechi de fire.

Are denumirea echivalentă de cablu FTP (*Foil Twisted Pair*).

Este un cablu hibrid între UTP și STP, care nu are ecran pentru fiecare pereche de fire din cablu, dar prezintă ecranul de grup.

Impedanța caracteristică a unei perechi de cablu ScTP este de 100 sau 120 Ohmi.

Ecranul este eficient doar dacă este împământat la ambele capete și nu prezintă discontinuități.

Atenuarea specifică a cablului impune utilizarea repetoarelor de semnal pentru transmisii pe distanțe mai mari de 100 m.

La capete se montează conectori ScTP speciali, prin sertizare, respectând codul culorilor.

CABLUL COAXIAL este alcătuit dintr-un conductor metalic central ("firul cald"), strat izolator, ecran ("masă") și manta.

Poate avea mai multe dimensiuni, specificate prin diametrul conductorului central (d) și diamentrul interior al ecranului (D), exprimate în mm, ca raport d/D:

- mici: 1,2/3,5; 1,2/4,2; 1,8/6,4;
- medii: 2,6/9,4;
- mari: 5/18.

Cablurile coaxiale sunt utilizate în diverse domenii, întrucât atenuarea proprie pe unitatea de lungime este redusă comparativ cu cablul torsadat, interferențele electromagnetice sunt practic nule și se pot utiliza segmente de cablu cu lungimi mai mari față de UTP (185 m pentru cablul coaxial subțire; 500 m pentru cablul coaxial gros).

În rețelele de calculatoare Ethernet se poate folosi:

- cablul coaxial subțire (*thinnet*) de 3,5 mm (RG-58), de 50 Ohmi, care este deosebit de ușor, flexibil, ușor de instalat și ieftin, dar necesită condiții deosebite de împământare; se folosește în rețele 10Base2, cu conector BNC (*Bayonet Nut Connector*).

- cablu coaxial gros (*thicknet*) de 9,4 mm (RG-59), de 75 Ohmi, mai greu, mai rigid și mai scump, dar de bandă mai largă, este indicat pentru realizarea magistralei de date (*backbone*)

dintr-un LAN (10 Base 5). Se mufează cu conectori BNC sau "Vampir" fiind folosit în rețele 10Base5.

CABLUL OPTIC (*Fiber Optic Cable*) - alcătuit din mai multe fibre optice, uni- sau multimod, cu miez transparent (din material plastic sau sticlă), înveliș refractar (*cladding*) cu indice de refracție mai mic decât cel al miezului, manta (*Plastic Shield*), material de umplere (*Kevlar Reinforcing Material*), eventual un fir de inox pentru creșterea rezistenței mecanice, și manta exterioară (*Outer Jacket*) din plastic.

Pentru rețelele de calculatoare se utilizează cablu optic dual, cu doar două fibre optice, care în funcție de dimensiuni (10 μ; 50 μ ... 100 μ) pot avea unul sau mai multe moduri de propagare a luminii în interiorul miezului.

Fibrele optice subțiri sunt de tip unimod și având o atenuare scăzută, sunt folosite pentru transmisii la distanțe mari fără amplificare (< 5km).

Fibrele optice groase sunt de tip multimod (de exemplu, 62,5/125μ sau 50/100μ) au atenuare mai mare și viteză redusă comparativ cu fibrele unimod, ceea ce limitează lungimea maximă a segmentului de cablu la cel mult 2 km.

Joncțiunile cablurilor trebuie realizate cu precizie, pentru reducerea pierderilor de semnal, și protejate cu optocuploare. La capete se montează conectori speciali (ST, SC, SMA).

Cablurile optice sunt folosite în rețele Ethernet (10 Base F), Fast Ethernet (100 Base F) și FDDI.

Conectorii pentru cablurile care conectează echipamente identice sunt realizați în varianta **inversoare**, cu încrucișarea firelor (*cross-connection*) astfel încât să se lege ieșirea datelor (TxD - *Data Transmission*) dintr-un echipament cu intrarea de date (RxD - *Data Receiving*) de la celălalt capăt. În documentațiile tehnice ale echipamentelor sunt specificate modurile de realizare a conectorilor pentru DTE (*Data Terminal Equipement*) și DCE (*Data Circuit Equipement*), cu numerotarea și semnificațiile pinilor și modul de conectare a conductoarelor din cablu pe baza codului culorilor.

În general, conexiunile între conectori diferiți sunt realizate pe baza unor diagrame care precizează pinii corespondenți.

Alte tipuri de conectori sunt:

- conectori DB-k sau D-k (modular cu k = 9; 15; 25; 37; 50; 68 pini, în forma literei D) pentru interfața Ethernet conectată fie la cablu torsadat, fie la cablu coaxial gros;
- conector universal AMPLIMITE 50 cu 50 de căi pentru diferite interfețe.

Orice conector poate fi asociat cu un anumit tip de magistrală (*bus*) de date. Denumirea unor conectori poate să precizeze și tipul bus-ului de date (de exemplu: D50 SCSI-2).

Prin standardul **SCSI** (*Small Computer System Interface*) se specifică un bus de 8 biți și tact de 5 Mhz, respectiv cu viteza de 5 MBps.

SCSI-2 sau **Fast SCSI-2** reprezintă o variantă de standard pentru bus de 8 biți și 10 Mhz frecvență de clock, cu 10 MBps viteză de transmisie a datelor.

Wide SCSI-2 este un standard îmbunătățit pentru bus de 16 biți, 5 MHz și 10 MBps.

Fast/Wide SCSI-2 definește un bus de 16 biți, 10 MHz și 20 MBps.

Ultra SCSI-2 standardizează un bus de 32 de biți, 10 MHz și 40 MBps. Se utilizează un canal secundar de transfer.

Alte standarde folosite pentru magistralele de date sunt următoarele:

ISA (*Industry Standard Architecture*): 16 biți, 8MBps.

EISA (*Extended ISA*): 32 biți, 33 MBps.

MCA (*Micro Channel Architecture*): 32 biți, 20 MBps.

PCI (*Peripheral Component Interconnect*) v2.0: 64 biți, 264 MBps.

AGP (*Advanced Graphics Card*) de 2x și 4x mai rapid ca PCI (pentru aplicații grafice).

PCMCIA (*Personal Computer Memory Card International Association*) sau simplu PC *Card* v3.0: 32 biți, 20-33 MHz, max. 132 MBps.

Sunt necesare adaptoare pentru interconectarea bus-urilor realizate în standarde incompatibile (de exemplu, adaptor PCI/SCSI).

Interfața AUI (*Attachment Unit Interface*) cu conector DB-15 poate fi utilizată pentru conectarea unui echipament fie la un cablu Ethernet, fie la un sistem cu transmisie radio (*wireless*), prin intermediul unui **transceiver** (transmițător/receptor - *transmitter/receiver*), având capacitatea de a detecta coliziunile. Un transceiver este utilizat pentru conectarea unui anumit echipament dintr-o rețea locală (calculator, router ș.a.) la mediul de transmisie (cablu UTP, coaxial, optic etc), prin intermediul unor interfețe AUI sau MII (*Media Independent Interface*). Un transceiver este un dispozitiv multiport care conține etaje de amplificare și convertoare de semnal (de exemplu, semnalul electric poate fi convertit în undă luminoasă și invers folosind diode LASER și fotodiode).

Lungimea unui segment de cablu este limitată din cauza fenomenelor specifice de atenuare și defazare a semnalelor pe liniile de transmisie. Pentru conexiuni la distanțe mai mari decât cea maxim admisă, se utilizează mai multe segmente de cablu interconectate prin intermediul **repetoarelor** care refac forma rectangulară a impulsului de formatare a datelor eliminând astfel efectele zgomotelor și distorsiunilor de transmisie, după care amplifică semnalul până la nivelul de referință. Există limitări privind numărul maxim de repetoare care pot fi intercalate între două noduri ale rețelei.

Un **repetor** este un diport care interconectează segmente de LAN diferite, cu diverși conec-

tori: 10 Base T (RJ-45), 10 Base 2 (BNC), 10 Base F (ST) sau cu alte medii fizice de transmisie prin intermediul AUI folosind transceivere. Acesta nu trebuie confundat cu un dispozitiv de conversie între două medii fizice diferite de transmisie, întrucât suplimetar, în repetor, sunt regenerate cadrele de date (de exemplu, Ethernet), în baza unor secvențe de sincronizare și sunt procesate informațiile privind posibilele coliziuni din rețea.

Convertorul de mediu face trecerea de la un tip de mediu la altul, prin conversia semnalului dintr-un format în altul.

Există convertoare pentru interconectarea a diferite tipuri de rețele, cum ar fi:

- rețea Ethernet de cablu UTP cu una cu cablu coaxial;
- rețea Ethernet pe cablu torsadat cu una cu transmisie pe fibră optică;
- rețea pe fibră optică multimod (MMF - *Multi Mode Fiber*) cu una pe fibră optică unimod (SMF - *Single Mode Fiber*);
- rețea de 10 Mbps cu un cablu de 100 Mbps.

Porturile de intrare-ieșire și conectorii aferenți sunt de tipuri diferite, în funcție de mediul fizic de transmisie.

IV.2 INTERFEȚE DE COMUNICAȚIE

Prin **interfață** este desemnat un modul, fizic (*hardware*) sau logic (*software*), prin intermediul căruia se realizează comunicația dintre echipamente și medii fizice sau dintre două procese logice.

Interfața este cea care controlează comunicația și asigură transmisia și recepția datelor în formatul standard adoptat. Datele intră sau ies dintr-un echipament numai prin intermediul unei interfețe. În funcție de nivelele OSI pe care lucrează interfața, aceasta se implementează fizic sau logic.

Implementarea fizică a unei rețele locale impune instalarea pe fiecare calculator a unei interfețe sau plăci de rețea (NIC - *Network Interface Card*), internă sau externă, cu programul aferent (*driver*), montarea cablurilor de legătură cu anumiți conectori, realizarea conexiunilor cu unitatea care centralizează traficul, desemnată prin diferiți termeni (MAU, CU, hub, LAN switch, concentrator, repetor etc) și instalarea pe server a sistemului de operare al rețelei (NOS - *Network Operating System*).

În figura IV.1, este exemplificat foarte simplu modul de realizare a unui LAN cu un calculator de tip server și un hub. Rețeaua se poate extinde prin utilizarea tuturor porturilor din hub.

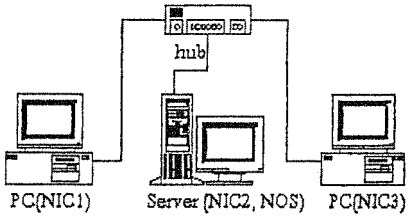


Fig.IV.1 Interconectarea echipamentelor într-un rețea

Rolul plăcii de rețea este acela de a asigura calculatorului accesul la serviciile oferite de rețea. Placa de rețea a server-ului asigură, în general, viteze mai mari de transmisie decât cele ale clienților din rețea. O placă de rețea lucrează pe subnivelul MAC, deci tipul ei depinde de arhitectura rețelei. Alegerea unei plăci de rețea se face în funcție de tipul bus-ului de date la care se va conecta (ISA, EISA, PCI, SCSI, PCMCIA etc) dar și de mediul fizic de transmisie (cablu sau "wireless"), fiind necesară o anumită interfață și anumiți conectori de legătură.

Interconectarea unui echipament cu mediul fizic de transmisie se face prin intermediul unei **interfețe fizice**, de nivel OSI 1 (*phisical interface / L1 interface*), denumită și **port fizic**.

Un echipament de comunicație (hub, switch, bridge, router etc) are mai multe porturi de intrare-ieșire, deci mai multe interfețe fizice care nu sunt neapărat toate de același tip.

În funcție de modul de comunicație adoptat (sincron/asincron, echilibrat/neechilibrat) se pot utiliza diferite tipuri de interfețe fizice definite prin standarde: RS-232 (V.24), X.21, V35, G.703 etc.

RS-232, standardizată de EIA (*Electronics Industry Association*), specifică toate caracteristicile electrice pentru transmisii seriale de date, sincrone și asincrone, de mică viteză.

EIA a realizat standardul RS-232-C pentru comunicații seriale iar CCITT a adoptat un standard echivalent, numit V.24. Este un standard pentru nivelul fizic de comunicație. Distanța maximă dintre DTE și DCE este de 16,5 m la un debit binar maxim de 19200 bps cu transmisie neechilibrată (se utilizează un singur fir de masă). Se utilizează conectori cu 25 de pini (DB-25) corespunzând la 25 de funcții specifice. RS-232-D se deosebește de RS-232-C prin circuite suplimentare de testare (la distanță sau în buclă locală).

Aceste standarde se pot utiliza pentru transmisii sincrone sau asincrone, pe 2 sau pe 4 fire, pe linii specializate sau în rețeaua telefonică comutată.

Nivelele de semnal sunt +3V...+15V pentru valoare logică '1', respectiv -15V...-3V pentru '0' logic.

Pentru **transmisii asincrone**, sunt utilizați efectiv doar 10 pini (9 pini dacă se folosește un

singur fir de masă), minimum 4 pini (cei specificați prin *):

1* - masa de protecție (**PG** - *Protective Ground*);

2*- transmisie de date (**TxD** - *Data Transmission*);

3*- recepție date (**RxD** - *Data Receiving*);

4- cerere de emisie (**RTS** - *Transmission Request*);

5- gata de emisie (**CTS** - *Clear To Send*);

6- DCE pregătit pentru transmisie (**DSR** - *Data Set Ready*);

7*- masă de semnal (**SG** - *Signal Ground*);

8- detecția purtătoarei (**CD** - *Carrier Detect*);

20- terminal de date pregătit (**DTR** - *Data Terminal Ready*).

Temporizările între semnalele de control depind de tipul circuitelor interconectate precum și de linia folosită pentru transmisie (de exemplu: timpul de comutare OFF-ON între pinii 4 și 5 este de 400-1000 ms pe linii comutate și de 20-50 ms pe linii închiriate).

Pentru **transmisii sincrone**, se utilizează suplimentar semnale de bază de timp, pe frecvența modem-ului (DCE), la emisie pinul 15, respectiv 17 pentru recepție. Dacă DTE este un port al unui calculator atunci tactul este transmis către DCE pe pinul 24.

Confirmarea sau infirmarea recepției corecte în regim semiduplex se poate face pe un canal auxiliar de mică viteză (tipic 75 bps).

Să exemplificăm primele faze ale unei comunicații între două DTE-uri prin intermediul unor modemuri cu interfețe RS-232.

Înaintea apelului propriu-zis apare comunicația dintre fiecare DTE și DCE-ul asociat, fiind activi (ON) pinii DTR și DSR (Fig. IV.2).

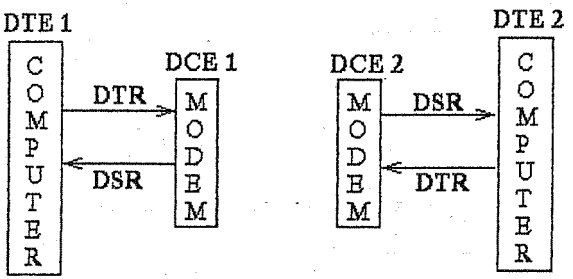


Fig.IV.2 Echipamente pregătite pentru transmisie

Cererea de transmisie a computerului 1 determină activarea altor pini înainte de a se realiza transmisia propriu-zisă a datelor (Fig. IV.3).

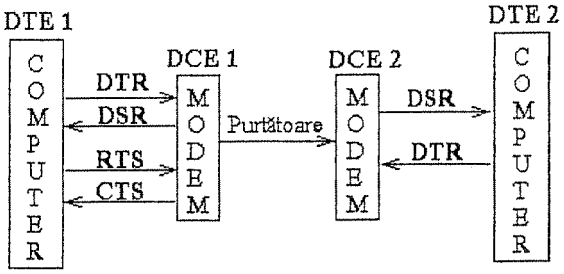


Fig. IV.3 Inițierea apelului

Modem-ul apelat sesizează prezența purtătoarei pe linie și activează CD spre terminalul 2 (Fig. IV.4).

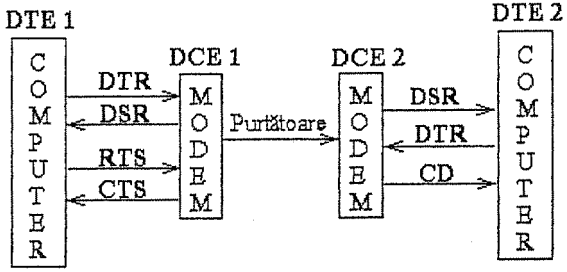


Fig.IV.4 Sesizarea apelului

Dacă terminalul apelat este pregătit să recepționeze datele, în prealabil va răspunde apelului prin transmisia pe linie a unei purtătoare de o anumită frecvență spre terminalul apelant (Fig.IV.5).

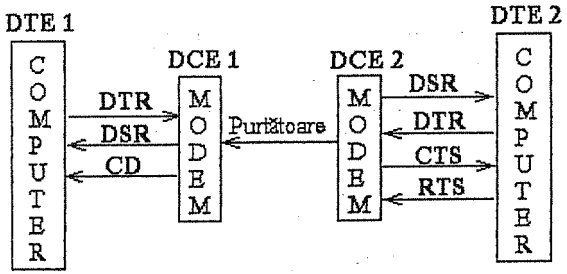


Fig. IV.5 Răspuns la apel

Se observă că transmisia se realizează în modul semiduplex, fiind necesară schimbarea sensului de transmisie pe linie, de mai multe ori în timpul comunicației.

La viteze mai mari de transmisie (48, 56, 64 kbps) se pot aplica standardele CCITT V.35, V.36, V.37, V.90 care prevăd circuite de date echilibrate.

Interfața RS-232-C a fost devansată prin standardul RS-449 care cuprinde **trei standarde**:

- RS-423-A, echivalent cu RS-232-C cu transmisie neechilibrată;
- RS-422-A cu transmisie echilibrată și fire duble în circuitele principale cu viteze de 10 Mbps la 130 m. (Zona de tranziție între nivelele logice este redusă de la 6 V la 0.4 V cu nivele absolute de maxim 6 V);
- RS-449 pentru specificarea caracteristicilor mecanice, funcționale și procedurale.

Interfața RS-449 utilizează doi conectori de legătură, cu 37 și respectiv 9 pini.

Se utilizează conectori modulari DB9, DB15, D25, DB37, D50.

Complexitatea acestui standard l-au făcut neatractiv pentru producători ceea ce a determinat înlocuirea lui cu RS-530 care lucrează cu un conector universal de 25 pini și prezintă aceleași structuri pentru circuitele de date, control și tact ca la standardele precedente cu diferența că lucrează numai în regim echilibrat, iar ca circuite de test se păstrează cele în buclă locală sau la distanță, precum și modul de test.

Standardele prezentate nu au posibilitatea de **apel automat.** S-au dezvoltat pentru comunicațiile în rețea telefonică publică comutată (PSTN - *Public Switched Telephony Network*) standardele RS-366-A și V.25. Folosirea modemurilor inteligente reduce însă atractivitatea acestora.

Pentru transmisii seriale digitale, CCITT a propus standardele X.21 și X.21bis pentru interfețele fizice utilizate în transmisii sincrone de date de mare viteză (10 Mbps), care lucrează cu un conector cu 15 pini (DB-15) sau universali (AMPLIMITE-50), cu semnale suplimentare de sincronizare de bit și de octet, pe distanțe de maxim 10 m. Costul interfeței X-21 este însă o problemă ceea ce a determinat adoptarea lui X.21 bis cu conector de 25 pini, echivalent cu RS-232-C. Totuși funcțiile speciale suplimentare oferite de standardul X.21 (conectare rapidă, grup închis de utilizatori, redirecționarea apelurilor etc) îl fac atractiv pentru rețelele publice de date.

V.35 propus de CCITT este echivalent cu standardul RS-530 al EIA pentru transmisii seriale, echilibrate sau neechilibrate, de mare viteză (2 Mbps). Utilizează conectori DB-25.

Viteza de transmisie a datelor printr-o interfață RS-232 este de ordinul zecilor de kbps (maximum 38400 bps), în timp ce X.21 și V.35 admit viteze de ordinul Mbps.

Astfel, conexiunile de mare viteză, pe porturile prin care un LAN se conectează la WAN se folosesc interfețe în standard X.21 sau V.35.

G.703 este recomandarea CCITT care definește caracteristicile fizice și electrice ale unei interfețe cu viteze de transmisie de 2048 kbps. Este utilizată în sistemele PRI ISDN (*Primary Rate Interface for Integrated Standard Digital Network*) pentru transmisii simultane voce-date, dar nu numai.

Interfața dintre nivelul fizic și cel al legăturii de date este o **interfață de nivel 2** (*Layer 2 interface / L2 interface*). Denumirea acesteia este dictată de tipul rețelei sau de protocolul de comunicație folosit: ETH (*Ethernet*), IP (*Internet Protocol*), PPP (*Point-to-Point Protocol*), FR (*Frame Relay*) etc. Implementarea acestora se poate face atât în variantă hardware (exemplu: *eth*), cât și software (exemple: *ip, ppp, fr*). Standardele care definesc interfața de nivel 2 specifică formatul cadrului de date și impun constrângeri privind lungimea maximă de cadru care poate fi transmis. Plăcile de rețea sunt interfețe de nivel OSI 2.

Notarea interfețelor se face în diverse moduri. De exemplu, interfața pentru un port asincron este denumită simplu *port* iar pentru unul sincron se notează abreviat *syn.* La denumirea abreviată a interfeței se adaugă, de regulă, un indice care face distincția între mai multe interfețe identice definite pe același echipament (de exemplu: *eth0; eth1; ppp0; ppp4; fr5*).

Noțiunea de **port** este utilizată fie pentru a desemna conectorul fizic de legătură dintre un echipament și rețea, fie ca noțiune abstractă prin care se specifică demultiplexarea căilor în cazul transmisiilor pe canale cu acces multiplu.

De exemplu, dacă se transmit datele în sistem TDM (*Time Division Multiplexing*), atunci prin același port Ethernet, respectiv interfață *eth,* pot fi conectați la LAN mai mulți utilizatori, prin interfețe (porturi) logice de tip *ppp,* configurate logic.

Între nivelele superioare ale modelului OSI sunt definite diferite interfețe logice.

Pentru transmisii ISDN se folosesc interfețele fizice:

bri (BRI - *Basic Rate Interface*) cu două canale B ISDN de date (64 kbps) și unul D (16 kbps) folosit pentru management și controlul legăturii;

pri (PRI - *Primary Rate Interface*) cu 30 de canale B (64 kbps) și unul D extins (64 kbps).

Încapsularea datelor cu un anumit antet (*header*), în care se specifică tipul de protocol utilizat, se poate face în mai multe moduri chiar și pentru o singură interfață. De exemplu, o interfață ETH poate fi încapsulată cu sau fără secvența SAP dictată de SNAP (*SubNetwork Access Protocol*).

Este foarte important să se cunoască modul de încapsulare a datelor la nivelul interfețelor pentru a putea remedia anumite probleme care apar în rețea dar și pentru a stabili dacă echipamentele produse de diverse firme sunt compatibile și pot fi interconectate.

În transmisiile asincrone cu legături punct-la-punct nu se încapsulează datele. Apar doar biții de START și STOP necesari delimitării intervalului de transmisie.

Observații

1. Numeroase detalii privind standardizarea echipamentelor sunt specificate în recomandările RFC (*Request For Comments*).

2. Modul de supraveghere a stării interfețelor (*up; down*), altfel spus managementul lor, se realizează cu diverse MIB-uri (*Management Information Base*), în baza protocoalelor de management de rețea, conform prevederilor RFC, de exemplu, SNMP (*Simple Network Management Protocol*) descris în RFC 1157.

IV.3 REPETOARE MULTIPORT (HUB)

Unitatea centrală dintr-o rețea cu topologie fizică de tip 'stea' este denumită **MAU** (*Multistation Access Unit*) pentru o rețea Token-Ring și **hub** pentru alte tipuri de rețele.

Indiferent de denumire, această unitate este la bază un **repetor** digital de semnal, cu mai multe porturi de intrare-ieșire. MAU nu ia nici un fel de decizie logică, ignorând adresele și conținutul mesajelor, realizând doar transferul datelor ca șir de biți de la un port la altul. În terminologia OSI, un hub sau un MAU este un **dispozitiv de nivel fizic** sau **de nivel 1** (*Physical Layer Device/L1 Device*). Dacă amplifică semnalul, hub-ul este considerat **activ**, în caz contrar fiind vorba de unul **pasiv.**

Hub-ul este nodul central (*master*) dintr-o rețea "în stea" (Fig.IV.6).

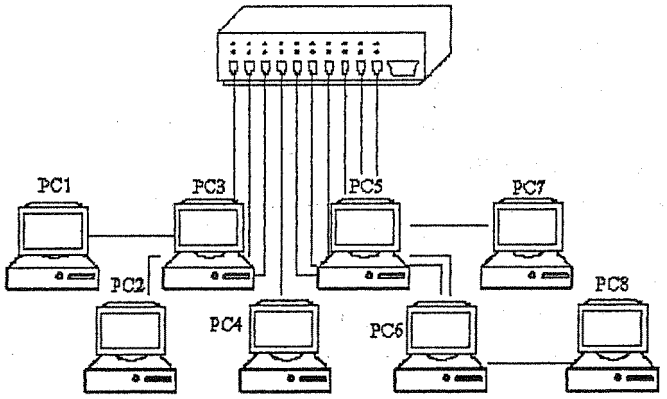


Fig.IV.6 Interconectarea calculatoarelor prin hub

Arhitectura LAN se poate baza fie pe principiul partajării benzii între toți utilizatorii (*media sharing*) folosind un **hub de partajare** (*Shared-Media Hub*), care lucrează ca un multiplexor TDM și limitează vitezele de transmisie la nivelul fiecărui nod în funcție de standardul adoptat (10Base2, 10BaseT, 100BaseT, 100BaseVG, ISO Ethernet etc), fie pe principiul legăturii punct-la-punct, cu un **hub cu matrice de comutație** (*Switched Hub*) care oferă pe fiecare port, unui singur calculator sau unui grup de calculatoare (segment de LAN), viteza maximă de transmisie. Avantajul arhitecturii cu matrice de comutație este acela că prin realizarea legăturii fizice dintre noduri, nu apar coliziuni și nu mai este necesară aplicarea unei metode specifice de acces la mediu.

Astfel devine posibilă transmisia duplex între nodurile rețelei rezultând arhitecturile:

1. *Full Duplex Ethernet* (20 Mbps);
2. *Full Duplex Token Ring* (32 Mbps);
3. *Full Duplex FDDI* (200 Mbps).

Din punct de vedere constructiv și funcțional, există trei categorii de hub-uri de partajare:

1. **Hub-urile simple** (*Standalone, Unmanaged* ori *Dumb Hubs*), cu/fără sursă proprie de alimentare, cu un număr fix de porturi, sunt neexpandabile și interconectează echipamentele dintr-o rețea cu arhitectură unică și mediu fizic de transmisie impus. Mai sunt denumite și **repetoare multiport**. Nu necesită configurare la instalare (fiind dispozitive *plug-and-play*).

2. **Hub-urile expandabile** (*Stackable Hubs*) admit folosirea algoritmi software pentru managementul echipamentelor rețelei (MIB) pe baza unui anumit protocol, de exemplu, SNMP. Aceste hub-uri au caracteristicile de bază ale hub-urilor simple (arhitectură unică de rețea, mediu fizic unic), dar pot fi puse în cascadă pentru realizarea unui hub virtual cu număr mare de porturi. Cascadarea hub-urilor este permisă pentru rețelele Ethernet de 10 Mbps (maxim 4 hub-uri, conform **regulii Ethernet 5-4-3-2-1**), dar nu se utilizează în rețelele Fast Ethernet deoarece lungimea maximă a cablului dintre hub-uri ar trebui să fie de 5 metri.

Cascadarea, realizată prin intermediul portului *up-link* utilizat pentru conexiunea cu nodul ierarhic superior, nu trebuie confundată cu stivuirea hub-urilor, unde legătura între acestea se realizează pe porturile pentru cablu UTP.

3. **Hub-urile inteligente** (*Managed Hubs*) sau **concentratoarele modulare,** numite simplu și **concentratoare**, prezintă o structură (*rack*) cu una sau mai multe surse de alimentare redundante, eventual un UPS (*Uninterruptible Power Supply*), o rețea proprie de cabluri de tip 'coloană vertebrală' (*'backbone in a box'*) la care se conectează modulele care leagă segmente de LAN cu arhitecturi diferite (Ethernet, Token Ring, FDDI) și medii fizice diverse. Modulele pot fi introduse în șasiu și în timpul funcționării hub-ului, adică 'la cald' (*hot-swappability*). În aceste hub-uri pot fi incluse și echipamente de interconectare a LAN-urilor pentru realizarea unei rețele de arie largă

echipamente de interconectare a LAN-urilor pentru realizarea unei rețele de arie largă (bridge, router etc), dar și module de securizare a transmisiei cu funcții specifice de criptare și autentificare.

În funcție de tipul și numărul porturilor din hub, acesta poate fi de tip:

1. **Minihub** - interconectează un număr redus (4;8) de utilizatori cu UTP. Unul din porturi permite conexiunea directă cu un alt hub sau switch, în vederea cascadării. Folosește o sursă externă de alimentare (PSU - *Power Supply Unit*), de 230V(Europa) sau 240V(UK).

2. **Microhub** - are aceleași caracteristici cu un minihub dar, suplimentar, este prevăzut cu porturi adiționale pentru conexiuni cu BNC sau AUI pentru fibră optică.

3. **Hub multiport** - are un număr mai mare de porturi (12; 24) pentru conexiuni UTP, BNC/AUI și poate fi folosit pentru rețele 10Base2 'în stea', cu cablu coaxial subțire. Un astfel de hub este prevăzut cu un modul SNMP și poate fi expandat prin stivuire, până la o limită superioară impusă (de exemplu, maxim 5 sau 6 hub-uri în stivă).

Observații:

1. Toate rețelele implementate cu cablu torsadat sau fibră optică folosesc hub-uri pentru partajarea resurselor sistemului.

2. Pentru o mai eficientă supraveghere a funcționării hub-ului, acesta este prevăzut cu LED-uri de diagnosticare, pentru urmărirea funcționării porturilor și a sursei de alimentare, eventual a legăturii cu rețeaua (*network load*).

3. Există așa-numitele **hub-uri rapide** (*Fast Hubs*) pentru rețele Fast Ethernet de 100Mbps. Utilizarea acestora este justificată în cazul transferului de fișiere de mari dimensiuni, cu o frecvență relativ redusă, dar folosirea lor nu avantajează transferul a foarte multe pachete mici.

4. Există hub-uri duale (*Dual Speed Hub*) care pot interconecta utilizatori de 10 Mbps și 100 Mbps.

5. Alegerea unui anumit tip de hub trebuie făcută în funcție de caracteristicile traficului din rețea. Dacă majoritară este comunicația dintre server și clienți, atunci un hub partajat este suficient. Dacă în rețea există mai multe servere sau comunicațiile dintre clienți predomină, atunci este indicat să se utilizeze un **hub cu matrice de comutare** (*Switched Hub*).

Matricea de **comutare spațială** funcționează similar cu cele din sistemul telefonic (PSTN - *Public Switching Telephone Network*), realizând conexiuni fizice dedicate, sigure, pe durata comunicației între două noduri. Un exemplu de comutator spațial Banyan sincron, în 3 trepte, este prezentat în figura IV.7.

Comutatorul din figură are 8 linii de intrare și 8 linii de ieșire. Fiecare celulă deplasează datele de pe un port de intrare pe portul de ieșire determinat de bitul de cale (0 sau 1). Bitul de cale cel mai semnificativ este citit primul, urmând apoi ceilalți biți. În figura IV.7.b este prezentată

calea de transfer a datelor de pe portul 4 de intrare, pentru secvența de cale 011. Se observă pentru transmisii simultane, posibila coliziune dintre această cale și cea definită de secvența 0 1 0 cu intrare pe portul 6, întrucât ambele ies în treapta a doua pe același port.

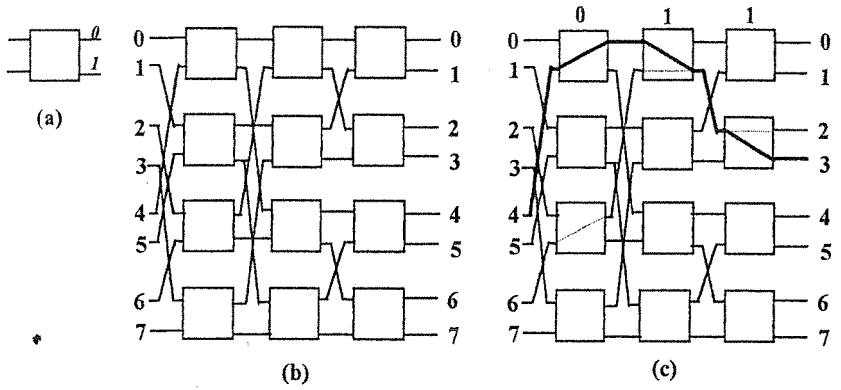


Fig. IV.7 (a) Celulă de comutare cu două porturi de intrare și două de ieșire;
(b) Comutator Banyan cu 8x8 în trei trepte;
(c) Trasee în comutatorul Banyan.

Această matrice de comutație spațială asigură legături simultane, fără coliziuni, între porturile similare de intrare-ieșire: 0-0 cu secvența de cale 000, 1-1 cu secvența 001, 2-2 cu secvența 010 etc. Există și alte soluții pentru comutarea de pachete.

Sistemul de comutație spațială diferă de cel de **comutare de mesaje**, specific poștei electronice (*e-mail*), care preia mesajul în întregime, îl stochează în memorie și apoi îl transmite către destinație (*store-and-forward*), fără să existe o legătură fizică între aceasta și sursă. Ineficiența utilizării legăturilor dedicate precum și capacitatea mare de memorie necesară comutării de mesaje sunt dezavantaje eliminate de **comutarea de pachete** care fragmentează mesajele în pachete mai mici, transmise către destinație pe căi diferite.

IV.4 COMUTATOARE DE REȚEA (SWITCH)

Dezavantajul hub-urilor de partajare este acela că nu elimină restricția ca numai un singur nod al rețelei să transmită la un moment dat, aplicând o anumită metodă de acces la mediul fizic. De aceea, producătorii de echipamente pentru rețelele de calculatoare au introdus matricile de comutație specifice centralelor telefonice (PBX - *Public Branch eXchange*) în comunicațiile de date, pentru realizarea în paralel a mai multor legături punct-la-punct simultane și evitarea

congestiilor. Astfel s-au obținut hub-urile cu matrice de comutare (*Switched Hubs*) sau **comutatoarele pentru LAN** (*LAN Switch*).

Conexiunile paralele, simultane dintre mai mulți utilizatori ai rețelei de calculatoare sunt create asemenea legăturilor virtuale telefonice folosind matrici de comutare.

Echipamentele care realizează comutarea cadrelor sunt denumite simplu **comutatoare de rețea** (*switch*) și sunt utilizate în rețele LAN cu diverse arhitecturi (Ethernet, Token-Ring, FDDI, Fast Ethernet), dar și pentru transmisiile în sisteme ATM (*Asynchronous Transfer Mode*) pentru comutarea semnalelor digitale de tip voce, audio sau video, la viteze foarte mari (de ordinul Gbps). În WAN, se utilizează comutatoare de mare viteză, cu capacități superioare celor pentru LAN.

Avantajele utilizării unui switch sunt evidente:

1. Prin intermediul switch-ului, se poate extinde rețeaua, structurată relativ simplu, fizic sau logic (rețele locale virtuale VLAN - *Virtual LAN*).

2. Reduce încărcarea rețelei prin filtrarea traficului.

3. Poate interconecta segmente de LAN cu medii fizice și viteze de transmisie diferite (10BaseT, 10BaseF, 100BaseT).

4. Permite utilizarea sistemelor de priorități pentru transmisie, prin introducerea în cadru a unui factor de calitate (QoS - *Quality of Service*).

În funcție de complexitatea operațiilor efectuate de switch, acesta poate lucra:

- pe nivelul OSI 2 al legăturii de date, mai precis pe subnivelul MAC sau pe LLC;
- pe nivelul 3 de rețea;
- pe nivelul 4 de transport.

Un **switch de subnivel MAC** (*Cut-through switch*) citește adresa MAC a destinației unui cadru și pe baza unui tabel de adrese (memorat pe durata procesului de "învățare" - *learning*), realizează legătura punct-la-punct dintre portul de intrare și cel de ieșire și expediază pachetul (*forwarding*). Decizia de comutare se poate lua și pentru fragmente foarte mici de pachete (sub 64B). Evident transferul este foarte rapid, dar este posibil ca acel cadru să fie afectat de erori și nodul-destinație să solicite retransmisia lui. Astfel rețeaua este folosită ineficient prin transmisia unui cadru eronat precum și a cererii de retransmisie.

Acest tip de switch este indicat în transmisiile în care se impun întârzieri mici de transmisie, fără un control strict al erorilor.

Un **switch de subnivel LLC** (*Store-and-forward switch*) citește cadrul primit, îl memorează și testează secvența FCS pentru detecția eventualelor erori. Dacă nu au apărut erori, cadrul este transferat către portul corespunzător destinației (Fig. IV.8) Acest switch realizează mai lent transferul decât unul de subnivel MAC, dar nu încarcă inutil rețeaua. Acest switch lucrează pe

momentul de decizie în switch-ul de subnivel LLC

Preambul 7 octeți	Câmp de START 1 octet	Adresa destinație 2 sau 6 octeți	Adresa sursă 2 sau 6 octeți	Câmp de lungime 2 octeți	Câmp de date LLC IEEE 802.2 46 - 1500 octeți	Câmp de control a erorilor (FCS) 4 octeți

momentul de decizie în switch-ul de subnivel MAC

Fig. IV.8 Momentele la care se ia decizia de comutare

același principiu cu 'punțile' de rețea (*bridge*), folosite pentru interconectarea mai multor rețele locale.

Pentru creșterea vitezei de funcționare a **switch**-ului **de nivel 2**, s-a propus o soluție de compromis (*Error-free cut-through switch*), un switch care în mod normal lucrează rapid, pe subnivelul MAC și numai dacă pe o anumită cale se sesizează apariția unor erori, atunci portul de ieșire respectiv este reconfigurat să funcționeze pe subnivelul LLC pe un interval limitat de timp. Acest switch nu ia decizii de comutare înainte de a recepționa primii 64 de octeți.

Switch-ul de nivel 2 asigură conexiuni **transparente** față de nivelele OSI superioare, întrucât lucrează numai pe baza adreselor MAC și nu depinde de protocolul de rețea folosit. Viteza de comutare a pachetelor în switch-ul de nivel 2 este mare.

Interconectarea unor segmente de rețea cu viteze diferite (de exemplu, 10 Mbps și 100 Mbps), poate crea la nivelul switch-ului **erori de depășire** a capacității de memorie (*buffer overflow*), urmate de pierderea unor cadre de date.

Producătorii de echipamente au propus diferite soluții pentru această problemă.

Prima constă în utilizarea unor memorii suplimentare dar determină creșterea costului echipamentului.

A doua soluție aplică procedeul de 'alarmă falsă', ca o reacție negativă, și nodul-sursă primește mesajul fals de apariție a unei coliziuni fiind forțat (*backpressure*) să oprească transmisia pe o durată aleatoare. Astfel se permite descărcarea memoriei până la transmisia de noi date dinspre nodul de mare viteză.

Un switch de nivel 2 poate fi utilizat în diferite rețele (Ethernet, Token Ring, FDDI, Fast Ethernet, ATM), cu diverse medii fizice de transmisie. Numărul porturilor din switch și cel al adreselor MAC admise pe fiecare port pot varia de la un echipament la altul. Unele porturi pot lucra în regim duplex cu condiția ca și placa de rețea (NIC) a echipamentului conectat la acel port să admită transmisia duplex a datelor.

Supravegherea funcționării unui switch este mai complicată decât a unui hub, întrucât trebuie urmărite mai multe legături punct-la-punct.

Există trei variante pentru realizarea managementului unui switch:

1. pe **principiul simplu al "oglinzii"** (*port mirroring*), se copie informația dintr-un port al switch-ului într-un analizor de LAN; numai un singur port poate fi monitorizat la un anumit moment;

2. pe **principiul "oglinzilor multiple"** (*multiple port mirroring*) se creează un sistem de monitorizare la distanță (RMON - *Remote Monitoring*), în mod aleator, la intervale regulate de timp, a unor grupuri de porturi din switch, dar tot numai câte unul la un anumit moment;

3. prin **sistemul RMON simultan** (*Simultaneous RMON View*) permite supravegherea simultană a traficului din mai multe porturi folosind un procesor (CPU - *Central Processing Unit*) separat doar pentru management și memorii suplimentare pentru a nu reduce performanțele switch-ului. RMON MIB este cea mai utilizată metodă pentru managementul switch-ului. Apar probleme în ce privește utilizarea simultană a RMON MIB și SNMP.

Există switch-uri de nivel 2 care admit utilizarea algoritmului de deducere a 'drumului minim' într-un graf (*Spanning Tree Algorithm*), în baza standardului IEEE 802.1d, asemenea routerelor.

Switch-urile **de nivel 3** (*L3 Switch*) combină avantajul vitezei mari de comutație a switch-ului de nivel 2 cu cele ale ruterelor (controlul traficului, deducerea rutei optime etc). Un switch de nivel 3 depinde de protocoalele de rețea utilizate.

Un astfel de switch realizează automat procesul de "învățare" a adreselor (*learning*) și construcție a tabelelor de comutare și rutare. Legăturile între diferite subrețele se realizează direct la nivelul de rețea. Nu se mai folosesc procesoarele RISC (*Reduced Instruction Set Computing*), ci cele ASIC. Funcțiile de rutare se realizează în baza anumitor protocoale de rețea, de exemplu, RIP (*Routing Information Protocol*); RIP II; OSPF (*Open Shortest Path First*); DVMRP (*Distance Vector Multicast Routing Protocol*). Aceste switch-uri lucrează ca routere rapide realizând rutarea la nivelul porturilor.

Switch-urile **de nivel 4** (*L4 Switch*) iau decizii de rutare evaluând informațiile de pe nivelul OSI 4 de transport, cum ar fi numerele porturilor logice (23 - port Telnet; 80 - port WWW etc), specificate de protocoalele de transport (de exemplu, TCP, UDP, SPX).

Observații:

1. Lățimea benzii oferite de un switch pe porturile active în paralel, devine suficient de mare prin folosirea standardelor de transmisie duplex și GbE (*Gigabit Ethernet*).
2. Întârzierile determinate de switch în procesul de transmisie a datelor devin importante în transmisiile de date în timp real (voce, audio, video).

IV.5 MODEMURI

Interconectarea echipamentelor terminale de date aflate la distanță necesită transmisia mesajelor prin anumite canale de comunicație respectiv diferite medii de transmisie (cu sau fără 'fir').

Rețeaua telefonică este deosebit de avantajoasă pentru comunicațiile de date datorită multitudinii utilizatorilor și a ariei extinse pe care o deservește. În zonele necablate sau cu forme de relief care fac accesul dificil, este avantajoasă folosirea sistemelor *wireless*.

Indiferent de mediul fizic de transmisie, se pune problema asigurării condițiilor optime de transmisie a datelor la distanță. Transmisia datelor în banda de bază, fără modulare/demodulare este permisă numai pe distanțe scurte. Accesul de la distanță a unui terminal neconectat permanent la o rețea locală este posibilă prin intermediul unui **modem** (*Modulator-Demodulator*).

Conversia datelor într-un semnal adecvat canalului de comunicații utilizat se face aplicând o anumită tehnică digitală de modulație (Tabel IV.1).

Există diferite tipuri de modem-uri:

- cu **cuplare directă** la canalul de comunicații, în particular cu conectare la priza telefonică sau cu transmisie prin undă radio în mediul *wireless*;
- cu **cuplare indirectă (acustică,** datele fiind transmise prin intermediul telefonului, mai precis a microfonului, sub formă de semnal acustic; **în infraroșu** - IRDA - *InfraRed Data Access*).

Evident modem-urile cuplate direct sunt mai performante dar pentru terminalele portabile (*laptop*) este avantajos un modem cu cuplaj indirect.

Modem-ul poate fi dispozitiv **extern,** independent de DTE sau modul în interiorul terminalului, adică modem **intern.**

În funcție de tipul canalului de comunicații folosit, modem-urile pot funcționa în regim:

- **simplex;**
- **semiduplex;**
- **duplex.**

Modul de transmisie diferențiază două categorii de modem-uri:

- **asincrone;**
- **sincrone.**

Un alt criteriu de clasificare a modem-urilor este lățimea benzii de frecvențe disponibile, rezultând modem-uri:

- **de bandă îngustă;**
- **de bandă largă.**

Tabel IV.1 Principalele tehnici digitale de modulație

Nr. ord.	Abreviere	Semnificație
1	ASK (DSB-SC-AM)	*Amplitude-Shift Keying (Double Side Band - Supressed Carrier - Amplitude Modulation)*
2	PSK (BPSK)	*Phase-Shift Keying; Binary PSK*
3	DPSK (DBPSK)	*Differential PSK*
4	DEPSK (DEBPSK)	*Differentially Encoded PSK*
5	QPSK (CQPSK)	*Quadrature PSK; Coherent QPSK*
6	OQPSK (SQPSK)	*Offset (Staggered)QPSK*
7	DQPSK	*Differential QPSK*
8	DEQPSK	*Differentially Encoded QPSK*
9	MSK(FFSK)	*Minimum-Shift Keying (Fast-FSK)*
10	DMSK	*Differential MSK*
11	GMSK	*Generalised (Gaussian) MSK*
12	SFSK	*Sinusoidal Frequency-Shift Keying*
13	GSFSK	*Generalised SFSK*
14	TFM	*Tamed Frequency Modulation*
15	Multi-h FM (Correlative FM)	*Multiple-Index FM*
16	IJF-OQPSK	*Intersymbol-Jitter-Free OQPSK*
17	TSI-OQPSK	*Two-Symbol-Interval OQPSK*
18	CPFSK	*Continuous-Phase FSK*
19	QAM	*Quadrature Amplitude Modulation*
20	SQAM	*Superposed QAM*
21	APK	*Amplitude Phase Keying*
22	QPRS	*Quadrature Partial Response Signal*
23	Q^2PSK	*Quadrature-Quadrature PSK*
24	GQ^{2}PSK	*Generalised Q^2PSK*

Modemurile telefonice pot fi proiectate:

- **pentru linii dedicate;**
- **pentru căi telefonice în banda vocală.**

Modem-urile de bandă largă (*broadband modem)* sau modem-urile **multiport** sunt în general utilizate pentru interconectarea mai multor terminale dintr-o rețea de comunicații, cu mediul de transmisie, în variantă multiplexată (Fig.IV.9). În aceste cazuri este necesară o bună sincronizare a DTE-urilor iar proiectarea și întreținerea acestor rețele sunt dificile. În plus, creșterea numărului de utilizatori devine o problemă.

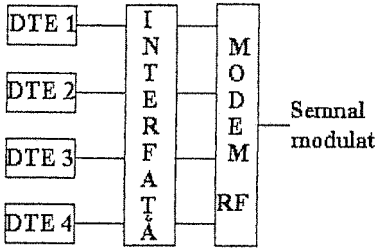


Fig.IV.9 Interconectarea componentelor unei rețele
de comunicații cu un modem de bandă largă

Standardele de transmisie în rețelele de comunicații de bandă largă stabilesc:

- lățimea benzii canalului de transmisie;
- numărul de canale;
- benzile de separare a canalelor;
- compatibilitățile cu alte standarde etc.

Modem-urile se caracterizează și prin **rata sau viteza de transmisie a datelor**. Prin compararea acesteia cu lățimea benzii alocate se obțin modem-uri:

- **de mică viteză;**
- **de mare viteză;**
- **de medie viteză.**

De exemplu, în cazul modemurilor telefonice, cu transmisie binară simplex sau semi-duplex în banda 300 Hz ... 3400 kHz, se consideră 9600 bps ca o viteză medie de transmisie iar 600 bps reprezintă o rată mică de transmisie. Transferul binar al datelor în mod duplex pe circuitele pe două fire se realizează pe o bandă de frecvențe redusă la jumătate comparativ cu transmisia pe patru fire.

Funcție de caracteristica atenuare-frecvență a liniei telefonice, dacă se utilizează o bandă îngustă de frecvențe: 800 Hz ... 2400 Hz, se pot transmite date fie cu un raport de puteri semnal/zgomot minim, fie pe distanțe mai mari (20 ... 30 km). Transmisia sincronă a datelor pe linia telefonică se poate realiza la viteze relativ mari de cel puțin 56 kbps.

Creșterea ratei de transmisie față de valoarea maximă impusă pentru transmisii binare, pe un canal de comunicații de bandă limitată, se poate face prin mărirea numărului stărilor modulatorului digital.

Performanțele tehnicilor digitale de modulație se exprimă prin următorii parametri:

- **Viteza (rata) de transmisie:** R [biți/s; bps];
- **Lățimea benzii de frecvențe** utilizate pentru transmisie: B [Hz];

- **Eficiența spectrală** (de bandă) :

$$\eta = \frac{R}{B} \text{ [biți/s/Hz]} \quad \text{(IV.1)}$$

- **Puterea în bandă:**

$$P_B = \int_{-B}^{B} W(f)df = 2\int_{0}^{B} W(f)df \text{ [W]} \quad \text{(IV.2)}$$

unde $W(f)$ este funcția **densitate spectrală de putere** a semnalului modulat.

Pentru o bandă oarecare specificată de frecvențe, se aplică relația de calcul a puterii:

$$P_{[f_1,f_2]} = 2\int_{f_1}^{f_2} W(f)df \text{ [W]} \quad \text{(IV.3)}$$

- **Puterea totală:**

$$P_T = \int_{-\infty}^{\infty} W(f)df = 2\int_{0}^{\infty} W(f)df \text{ [W]} \quad \text{(IV.4)}$$

sau, aplicând relația integrală a lui Parseval,

$$P_T = \int_{-T/2}^{T/2} |p(t)|^2 dt \quad \text{(IV.5)}$$

unde $p(t)$ reprezintă expresia în domeniul timp a impulsului formator a datelor.

În general, pentru uniformizarea puterii transmise se preferă normarea puterii totale a semnalului modulat la energia de simbol, prin introducerea unui factor de normare a amplitudinii impulsului de semnalizare.

- **Puterea în afara benzii:**

$$P_{out\ of\ band} = P_T - P_B \quad \text{(IV.6)}$$

poate fi calculată pentru o anumită valoare a parametrului B sau poate fi reprezentată grafic ca funcție de lățimea benzii canalului de transmisie.

Graficele densității spectrale de putere și a puterii în afara benzii constituie două caracteristici de frecvență deosebit de importante pentru orice semnal modulat.

- **Eficiența de putere:**

$$r = \frac{P_B}{P_T} \cdot 100\,[\%] \quad \text{(IV.7)}$$

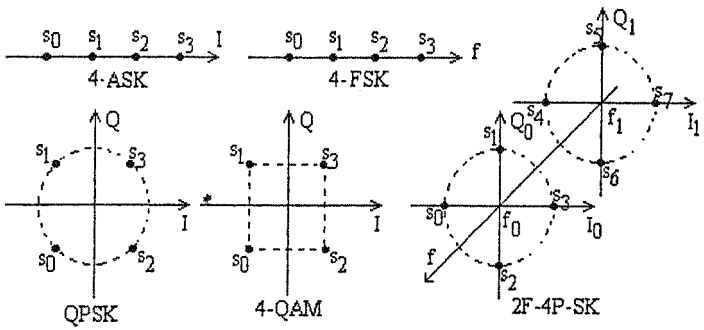
- **Banda** semnalului modulat o definim ca fiind lățimea benzii de frecvențe, măsurată unilateral în jurul frecvenței purtătoare, în care este inclusă o anumită cotă admisă (90%; 95%; 99%) din puterea totală a semnalului.

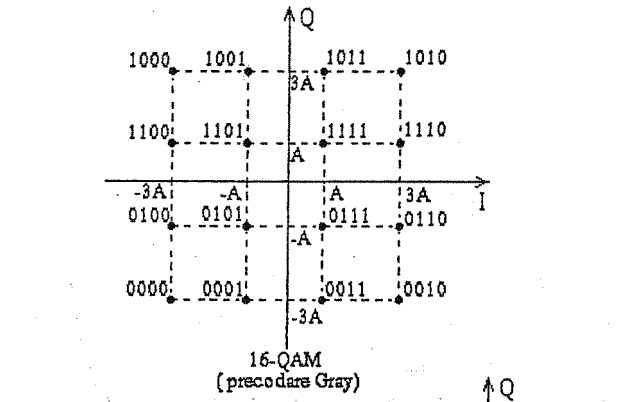
În cazul transmisiilor afectate de zgomot aditiv gaussian, o caracteristică importantă a modemului este cea a **probabilității de eroare** în blocul de decizie din receptor, ca funcție de raportul puterilor semnal/zgomot.

Expresia funcției probabilitate de eroare se deduce pe baza constelației de stări a semnalului modulat în planul semnalelor (Fig. IV.10), în funcție de natura și de mărimea perturbațiilor care afectează procesul de transmisie:

- zgomot aditiv, gaussian, alb sau colorat: AWGN - *Additive White Gaussian Noise*, ACGN

- *Additive Coloured Gaussian Noise*;
  - interferență intersimboluri (ISI - *InterSymbol Interference*);
  - interferențe cu alte canale;
  - zgomote de fază;
  - fading.





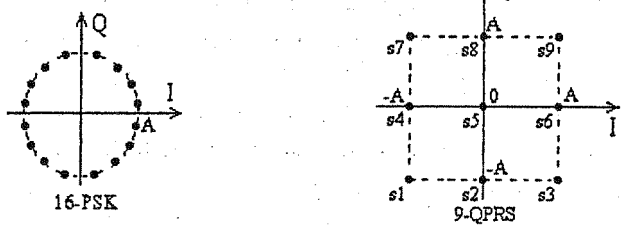


Fig.IV.10 Constelații de stări în spațiul semnalelor

Se preferă exprimarea probabilității de eroare ca funcție de raportul de puteri purtătoare/zgomot (C/N) în cazul modemurilor cu eficiență spectrală ridicată și ca funcție de raportul energie de bit/zgomot (E_b/N_0) pentru modemurile cu eficiență de putere.

Orice instrument care măsoară raportul C/N poate fi recalibrat pentru a măsura raportul E_b/N_0. Acest ultim raport este tot mai mult utilizat întrucât este o mărime normalizată, independentă de banda de zgomot a receptorului.

Între cele două rapoarte există relația:

$$\frac{E_b}{N_0} = \frac{C}{N} \cdot \frac{B}{R} = \frac{C}{N} \cdot \frac{1}{\eta} \qquad \text{(IV.8)}$$

Probabilitatea de eroare a demodulatoarelor digitale depinde și de caracterul coerent sau necoerent al acestora.

În tabelul IV.2 sunt prezentate valorile necesare ale raportului semnal/zgomot (S/N sau SNR - *Signal-to-Noise Ratio*) pentru un modem în cuadratură (QPSK) cu eficiență de putere și demodulare coerentă, în vederea obținerii anumitor performanțe de eroare la recepție.

TABEL IV.2

Valoarea necesară a raportului S/N

pentru o valoare impusă probabilității de eroare

P_e	S/N (dB)
10^{-2}	5,2
10^{-3}	7,3
10^{-4}	8,6
10^{-5}	9,8
10^{-6}	10,4
10^{-7}	11,3
10^{-8}	12,2

În figura IV.11 este reprezentat graficul probabilității de eroare ca funcție de raportul E_b/N_0 (energie de bit/d.s.p. a zgomotului alb aditiv) pentru semnal QPSK, cu anvelopă constantă, cu modulație de fază și cu eficiență de putere ridicată.

Cererile actuale de transmisie în sistemele de comunicații terestre (sisteme cu microunde, transmisii pe cablu sau fibră optică, sisteme de transmisii vocale) sunt în continuă creștere, astfel că se impune folosirea unor modemuri cu eficiență spectrală ridicată, respectiv viteză mare de transmisie și lățime minimă a benzii de frecvențe alocate. Noile generații de **modemuri cu eficiență spectrală** mare, cum ar fi cele de tip QAM, QPRS și TCM (*Trellis Coded Modulation*) cu număr mare de stări, asigură un coeficient de eficiență a benzii de cel puțin 6 biți/s/Hz.

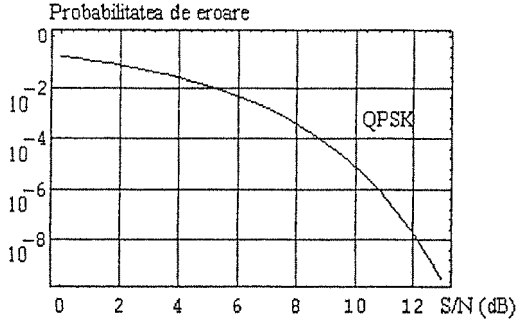


Fig.IV.11 Curba probabilității de eroare a semnalului QPSK

Tehnicile digitale de modulație utilizate frecvent în cazul echipamentelor de comunicații cu putere de emisie limitată și în comunicațiile radio mobile cu amplificatoare de putere neliniare, au un raport de puteri purtătoare-zgomot (C/N - *Carrier to Noise*) insuficient pentru a permite obținerea unei eficiențe spectrale ridicate. Acestea se numesc **modemuri cu eficiență de putere** și au limitată eficiența spectrală la maximum 2 biți/s/Hz. În categoria modemurilor cu eficiență de putere sunt incluse modulațiile pe purtătoare ortogonale cu anvelopă constantă (CE-QAM - *Constant Envelope QAM*) precum și tehnicile de modulație de frecvență cu continuitate de fază (CPFSK).

În figura IV.12 este prezentată schema-bloc a unui modem 256-QAM utilizat pentru transmisie pe canal T1 de 1,544 Mbps.

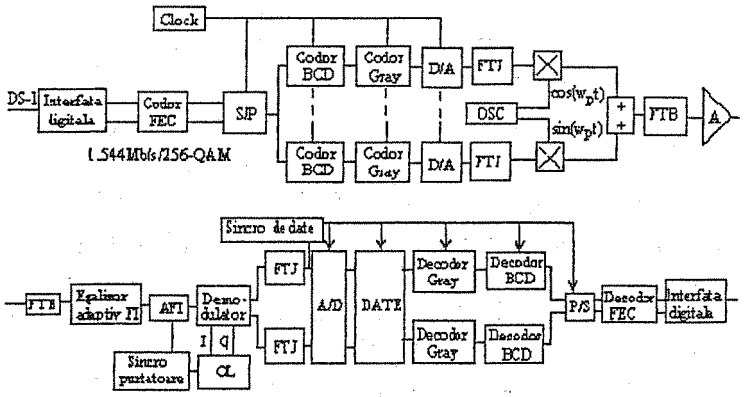


Fig.IV.12 Modem 256-QAM de 1,544 Mbps

Modemul are incorporate un filtru egalizor adaptiv în banda de bază (BATE - *Baseband Adaptive Transversal Equalizer*) și circuite de corecție a erorilor (FEC - *Forward Error Correction*), precum și circuite de sincronizare, amplificare și filtrare.

O altă posibilitate de optimizare a performanțelor modulatoarelor digitale de mare viteză constă în precodarea de tip **trellis** a semnalelor modulatoare în vederea creșterii distanței euclidiene dintre stările între care se efectuează tranziții. Acest lucru conduce la creșterea marginii de zgomot dintre stări, respectiv la scăderea sensibilității sistemului de comunicații față de zgomotele aditive. Se obțin așa-numitele **tehnici TCM** (*Trellis-Coded-Modulation*).

În tabelul IV. 3 sunt prezentate câteva tipuri de modem-uri telefonice și caracteristicile acestora.

Modemurile în standarde CCITT utilizează frecvențe de apel de 2100Hz; 2400Hz și 2250Hz în timp ce în standardele Bell Systems transmit apelul pe 2225 Hz.

Interconectarea a două modemuri realizate în standarde diferite implică asigurarea compatibilității lor ca valoare a frecvenței de apel, mod de transmisie, tip de modulație, viteză de transmisie etc. Compatibilitatea electrică este asigurată de interfața de comunicații (RS-232; RS-449; X.21 etc).

Observații

- Există anumite circuite denumite impropriu **modemuri în banda de bază** care realizează doar operațiile complementare unui modem privind procesarea datelor (codare, decodare, filtrare, egalizare, corecții de semnal, sincronizare de bit etc.). Deși nestandardizat de CCITT, acest tip de circuit poate fi folosit pentru transmisia datelor pe linii telefonice urbane, nepupinizate, la viteze de 1200, 2400, 4800, 9600 și 19200 bps.

Datele, sincronizate de tactul intern al modem-ului, sunt codate conform unui anumit cod de linie (Bifazic, Miller etc). Cuplarea terminalului de date la linia telefonică se face printr-un transformator de linie (interfață V.24).

La recepție, din semnalul egalizat cu un filtru adaptiv, se reface semnalul de date codat urmând a se face în final decodarea.

- Interconectarea DTE-DCE rspectiv calculator-modem se poate face printr-o interfață ce corespunde standardului de transmisie adoptat (CCITT V.24; RS-232-C; RS-422-A; RS-423-A; RS-449 ș.a.). În cazul folosirii interfeței seriale RS-232-C conexiunile se pot face pe un număr minim de pini (semnale: transmisie de date XMIT (2); recepție de date RECV (3); masă de semnal SG(7)) în cazul transmisiei neechilibrate, caz cunoscut sub denumirea de **conexiune simplă de modem nul** (Fig.IV.13).

Tabel IV.3 Modemuri telefonice (standarde CCITT)

Standard	Debit (bps)	Mod de transmisie		Modulație	Linie folosită
V.17	14400	sincron	semiduplex	TCM	comutată
V.21	300	asincron	semiduplex, duplex	BFSK	comutată
V.22	600	asincro sincron	semiduplex, duplex	BPSK	comutată/ închiriată
	1200	asincron sincron	semiduplex, duplex	DQPSK	comutată/ închiriată
V.22bis	1200	asincron	semiduplex, duplex	DQPSK	comutată
	2400	asincron	semiduplex, duplex	QAM	comutată
V.23	600	asincron sincron	semiduplex, duplex	BFSK	comutată
	1200	asincron sincron	semiduplex, duplex	BFSK	comutată
V.26	1200	sincron	semiduplex	BPSK	comutată
V.26bis; ter	2400	sincron	semiduplex, duplex	DQPSK convenția B	închiriată
V.27	7200	sincron	semiduplex, duplex	8-PSK convenția A	comutată/ închiriată
V.29	4800	sincron	semiduplex, duplex	QPSK	închiriată
	7200	sincron	semiduplex, duplex	8-APK	închiriată
	9600	sincron	semiduplex, duplex	16-APK	închiriată
V.32	4800	sincron	semiduplex, duplex	4-QAM	închiriată
	9600	sincron	duplex	16-TCM/ 16-QAM	comutată
V.32bis	max. 14400	sincron	duplex	128-TCM; (64-TCM; 32-TCM)	comutată sau linie pe 2 fire, închiriată cu legături PP;
V.33	14400	sincron	semiduplex, duplex	TCM	închiriată
V.36	48k, 56k 64k, 72k	sincron	duplex	AM-VSB	canal de grup primar (48kHz)
V.61	4800 ... max. 14400	sincron	duplex	TCM	comutată sau pe 2 fire, închiriată

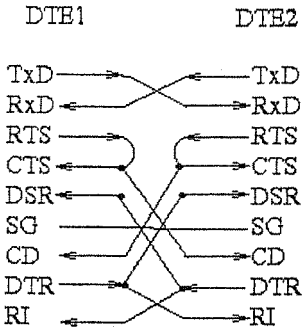


Fig.IV.13 Configurația completă a cablului de modem nul

Cele mai atractive din punctul de vedere al facilității de utilizare sunt **modem-urile inteligente** (*Smartmodems*) prevăzute cu **unitate de apel automat** (*ACU - Automatic Calling Unit*). Această unitate, realizată sub formă hard sau soft , este cea care plasează apelul pe linie și stabilește legătura, fie la anumite ore când tarifele de transmisie sunt mai mici, fie când numărul utilizatorilor este redus. Altă aplicație a unității de apel automat este cea de verificare a apelantului prin preluarea adresei acestuia și apelarea lui ulterioară în vederea eliminării posibilității preluării unor informații false de la potențiali adversari. Modem-urile inteligente lucrează cu secvențe de control speciale (exemplu: setul de instrucțiuni Hayes) pe baza unor protocoale specifice. Standardul RS-366 prevede caracteristicile ACU incorporate în modem-urile digitale.

Modem-urile inteligente Hayes sau 'compatibile Hayes' folosesc setul complet sau parțial de instrucțiuni Hayes, originale sau modificate, cu prefix AT și parametri exprimați binar (0 sau 1). Modificarea acestor comenzi a avut ca scop creșterea vitezei de lucru peste 9600 bps, valoarea specifică modem-urilor Hayes.

Setul de comenzi Hayes stă la baza programelor soft de control a modem-urilor cu unitate automată de răspuns și apel. Programul respectiv (*software*) oferă diferite opțiuni care vizează:

- tipul legăturii: poștă electronică (*e-mail*); transfer de fișiere (FTP); aplicații facsimil; transmisii vocale etc.
- monitorizarea continuității transmisiei cu sesizarea eventualelor întreruperi (*File Transfer in Progress*);
- operații de tip utilitar (*rename; delete; copy; paste);*
- setarea unor echipamente (imprimantă, scanner etc);
- efectuarea de teste de transmisie.

Compatibilitatea modemurilor inteligente trebuie asigurată la nivelul seturilor de comenzi de bază și rezultante, eventual și la nivel de registre.

Comunicațiile între modemurile inteligente sunt coordonate prin diverse protocoale.

Protocolul MNP (*Microcom Networking Protocol*) este destinat transferului de fișiere de date, între modem-uri inteligente, cu capacitate mare de detecție și corecție a erorilor de transmisie.

În prezent, acest protocol este utilizat ca standard industrial.

Proiectat după modelul OSI, protocolul MNP prezintă 3 nivele:

1. nivelul legăturii de date;

2. nivelul de sesiune;

3. nivelul de transfer de fișiere.

Formatul unui cadru MNP este asemănător celui utilizat de protocoalele SDLC și HDLC. Se folosesc câmpuri de delimitare (*FLAG*) de trei octeți. Primul câmp de control descrie utilizatorul (mod de transmisie duplex/semiduplex; lungimea mesajului etc) iar al doilea stabilește nivelul serviciului sau clasa protocolului MNP în care se efectuează transmisia. Controlul erorilor se face cu un cod ciclic (CCITT-12; CCITT-16 etc).

Protocolul MNP are 9 **clase de utilizare** dezvoltate succesiv:

Clasa 1 - transmisie asincronă, semiduplex, BOP (*Byte Oriented Protocol*);

Clasa 2 - suplimentar mod de transmisie duplex;

Clasa 3 - transmisie sincronă în pachet, fără biți de START și STOP;

Clasa 4 - se adaugă clasei 3 facilități de optimizare a formatului pachetelor și lungime adaptivă a grupelor de pachete de date;

Clasa 5 - se utilizează metode de compresie a datelor;

Clasa 6 - se negociază viteza de transmisie și se aplică transmisia duplex statistică (asemănător alocării dinamice a vitezelor de transmisie specifice protocolului WFQ utilizat în sistemele ATM);

Clasa 7 - se aplică metode de compresie a datelor cu predicție;

Clasa 8 - se adaugă în structura modem-ului filtre de egalizare realizate în standard CCITT V.29;

Clasa 9 - se combină avantajele modem-ului în standard CCITT V.32 cu metodele de compresie a datelor obținându-se debite binare de 40 kbps în transmisie duplex.

Observație

În momentul stabilirii legăturii între două terminale, protocolul consideră că acestea pot comunica doar pe nivelul logic inferior. După această etapă, urmează a se negocia clasa MNP în care se poate încadra transmisia respectivă, în funcție de performanțele

modem-urilor folosite. Astfel dacă un modem MNP întâlnește unul non-MNP, modem-ul MNP va lucra ca modem neinteligent făcând posibilă transmisia datelor.

Modem-ul asociat terminalului care inițiază transmisia, DCE-ul apelant, se găsește în **modul de transmisie** (*ORIGINATE*) iar cel care răspunde apelului și recepționează mesajul este în **modul de răspuns la apel** (*ANSWER*). Stabilirea propriu-zisă a legăturii cu echipamentul apelat se realizează în **modul de apel** (*DIAL-MODE*). Testarea funcționării modem-ului se face în **modul de autotest** (*SELF-TEST; LOOPBACK-TEST*) iar întreruperea procesului de comunicație în condițiile schimbării parametrilor de transmisie (atenuări puternice pe linie sau recepția unei secvențe 'nule' de tip *break-condition*) se poate face prin **deconectarea automată** a modemului (*AUTOMATIC DISCONNECT*).

Uzual, interconectarea DTE-ului cu un DCE se face prin intermediul unei interfețe care respectă un anumit standard de comunicație (RS-232-C, RS-449; RS-422-A; RS-423-A; EIA- 694; V.24; V.28 ș.a.) cu conectori cu număr diferit de căi (9; 25; 37). Tendințele actuale de transmisie a datelor între echipamente apropiate (2m), cu viteze relativ mari (Mbps), exclud legăturile 'pe fir', în favoarea celor *wireless* prin unde radio sau 'în infraroșu' (IrDA- *Infrared Data Access*).

Inversarea sensului de transmisie pe un canal cu comunicație în modul semi-duplex implică transmisia unor secvențe de control (de tip ACK; ENQ) nespecifice protocoalelor simple (ex. RS-232). Este necesară aplicarea unui protocol de transmisie pe un nivel superior, cum ar fi protocolul Bisync.

În anumite condiții se utilizează un canal suplimentar (secundar) de comunicații (*Backward Channel*) invers ca sens față de canalul principal, pentru transmisia unor secvențe de sincronizare, corecție de erori sau pentru controlul traficului.

Controlul funcționării modem-ului se face prin intermediul UART (*Universal Asynchronous Receiver-Transmitter*). În general, acesta admite un număr limitat de conexiuni prin modem și permite testarea unor condiții de transmisie prin **registrul de control a modem-lui** (MCR - *Modem Control Register*) precum și determinarea stării modem-ului prin **registrul de stare a modem-ului** (MSR - *Modem Status Register*).

MCR poate determina anumite întreruperi ale UART, poate activa semnalele DTR (*Data Terminal Ready*) și RTS (*Request-To-Send*) spre UART.

DTR activ semnifică faptul că terminalul propriu este conectat prin modem la linia telefonică.

RTS reprezintă cererea de transmisie în cazul comunicațiilor semiduplex.

Registrul de stare MSR este utilizat pentru sesizarea schimbărilor intervenite în funcționarea modem-ului. Orice modificare a stării modemului determină apariția unei întreruperi în

funcționarea UART prin **registrul de activare a întreruperii** (IER - *Interrupt Enable Register*) și cel de **identificare a întreruperilor** (IIR - *Interrupt Identifier Register*).

Testarea funcționării modem-ului se poate efectua în următoarele variante (Fig. IV.14):

- **autotest** (*Self-Test*): Modemul în buclă închisă este deconectat de la linie și de la terminalul propriu. O secvență binară de test, generată intern, este modulată și apoi demodulată. Se compară secvența obținută cu cea inițială. Se testează atât frecvențele de emisie cât și cele de recepție.
- **test de transmisie analogică** (*Analog Loopback Test*): se testează legătura modemului cu terminalul propriu conexiunea cu linia telefonică fiind întreruptă.
- **test de transmisie digitală** (*Digital Loopback Test*): se verifică funcționarea modem-ului apelat , terminalul propriu fiind deconectat.
- **test global** (*Remote Loopback Test*): sunt testate ambele modem-uri precum și linia telefonică.

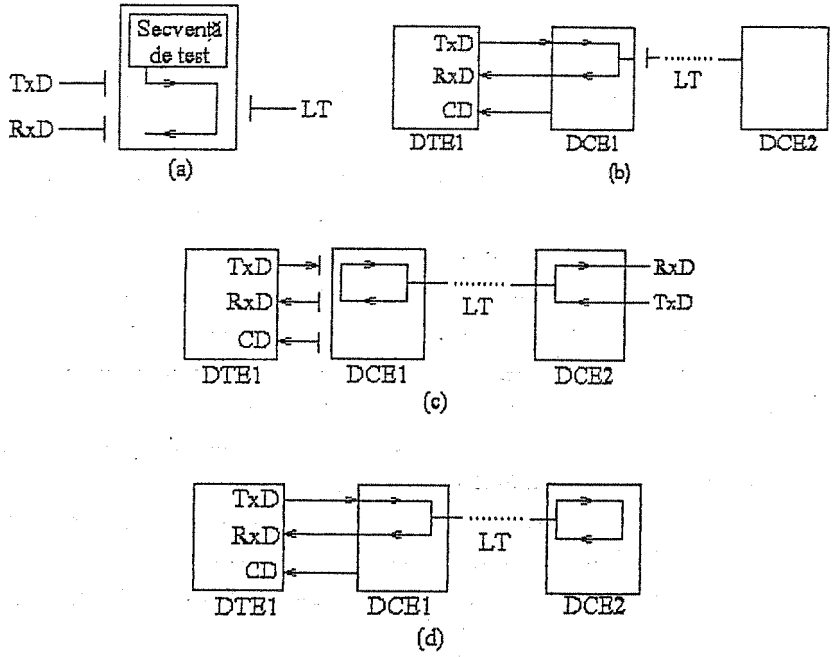


Fig.IV.14 Testarea modem-ului: (a) auto-test;
(b) testare analogică;
(c) testare digitală;

V

SISTEME DE OPERARE

V.1 GENERALITĂȚI PRIVIND SISTEMELE DE OPERARE

Orice PC funcționează pe baza unui program (*software*) denumit **sistem de operare** (OS - *Operating System*) care gestionează toate resursele sistemului, funcționând ca interfață între programele de aplicații și componentele fizice (*hardware*).

Sistemul de operare este instalat pe discul-fix (HDD - *Hard-Disk Drive*) al calculatorului, pe așa-numita partiție activă, și este încărcat la fiecare pornire a sistemului (*boot*) din memoria ROM (*Read-Only Memory*) de către BIOS (*Basic Input-Output System*) după testarea sistemului și identificarea unităților de disc (HDD, CDROM, floppy), a memoriei RAM (*Random Access Memory*) disponibile și a monitorului, pe baza informațiilor conținute în memoria CMOS (*Complementary Metal Oxid Semiconductor*).

Un sistem de operare este conceput ca un program care rulează în permanență în calculator, în timpul funcționării acestuia. De multe ori pentru OS se folosește termenul echivalent **kernel.**

Scopul principal al kernelului este acela de a oferi utilizatorului un mod transparent de comunicare cu calculatorul, adică posibilitatea execuției programelor utilitare fără a fi necesară cunoașterea detaliilor privind funcționarea părții hardware sau a nivelelor software inferioare celui de aplicație.

Simplificarea modului de accesare a programelor de aplicație este posibilă prin folosirea **interfețelor grafice de utilizator** (GUI - *Graphic Unit Interface*).

De asemenea, kernelul permite programatorilor de aplicații să lucreze cu un set standard de comenzi adresate acestuia, fără a recurge la comenzile codate specifice limbajelor-mașină, dependente de tipul de hardware sau de software folosit.

Un calculator este un sistem complex alcătuit din cinci subsisteme:

1. procesor (CPU - *Central Processing Unit*)
2. memorii
3. subsistemul de stocare a datelor
4. subsistemul video
5. magistrale (de date, de adrese etc).

La acestea se adaugă echipamentele periferice care reprezintă interfețele dintre utilizator și calculator (tastatură, mouse, monitor).

Frecvența de lucru a procesorului (*clock speed*) influențează direct performanțele calculatorului. Rapiditatea acestuia depind de cantitatea de memorie de mare viteză disponibilă în cipul procesorului (*on-chip/ primary/Level 1-cache memory*) și în afara acestuia (*off-chip/secondary / Level 2-cache memory*).

În ultimul caz este necesară o magistrală de date (*cache bus*) cu o anumită viteză de transfer și o anumită dimensiune (32; 64 biți), pentru comunicația dintre memoria cache primară și cea secundară.

Comunicația dintre componentele calculatorului se realizează pe diferite magistrale, externe sau interne, de diferite tipuri (ISA, EISA, PCI, AGP, SCSI, PCMCIA).

Kernelul administrează și alocă, la cerere (*system call*), diverselor programe de aplicații, resursele sistemului, precum:

- timp de procesare a unității centrale (CPU - *Central Processing Unit*);
- acces la memoria RAM;
- spațiu de stocare a datelor pe disc simultan cu administrarea sistemului de fișiere;
- resurse de intrare-ieșire.

Comunicarea dintre kernel și componentele hardware ale calculatorului se face prin intermediul unor programe software, de mici dimensiuni, de control a fiecărui echipament în parte (*device driver*), compatibile în general numai cu anumite sisteme de operare și cu un anumit tip de echipament. Funcționarea oricărei componente hardware din calculator este posibilă prin instalarea unui driver corespunzător.

Interacțiunea directă a sistemului de operare cu componentele hardware ale calculatorului se exercită prin intermediul **sistemului de întreruperi** (IRQ - *Interrupt ReQuest*) și prin **excepții,** adică acele evenimente neprevăzute (erori de sistem) pe care kernelul trebuie să le elimine. De exemplu, dacă un program încearcă să scrie în spațiul de memorie alocat altei aplicații, atunci kernelul intervine în soluționarea acestei excepții prin protejarea acelei zone și trimite un mesaj de eroare (*general protection fault*).

În fapt, sistemul de operare destinat clienților urmărește corectitudinea funcționării CPU, administrează spațiile de memorie și sistemul de fișiere (FS - *File System*) asigurând stocarea și recuperarea datelor pe disc, monitorizează procesele de intrare/ieșire și comunicațiile dintre procese, dar răspunde și de securitatea sistemului.

Programul utilizat de un calculator pentru a se conecta la o rețea locală se numește **program-client** (*client software*) iar stația respectivă reprezintă un **calculator-client** (*client-PC*). Clientul, software sau hardware, este cel care adresează o cerere către o componentă a sistemului. Răspunsul la cererea clientului este dat de o altă componentă denumită **server,** care reprezintă un furnizor de servicii. Natura serverului poate fi logică (*software*) sau fizică (o componentă *hardware* din sistem).

Comunicația dintre un PC și rețea este posibilă numai dacă sistemul local este compatibil, hardware și software, cu rețeaua. Din acest motiv, clienții și serverele dintr-o rețea trebuie să folosească același sistem de operare de rețea (NOS - *Network Operating System*), cum sunt NetWare, Windows NT etc. Există versiuni diferite de NOS, ca preț și complexitate, pentru client și pentru server.

În figura V.1, se prezintă interacțiunile dintre componentele unui sistem de tip client, sub forma unui model stratificat.

Între oricare două module software se intercalează interfețe logice cum sunt cele grafice GUI, cele de aplicație API (*Application Programming Interface*) etc.

Arhitectura sistemului de operare poate fi concepută fie în variantă **monolitică,** ca un sistem închis, dificil de modificat sau de îmbunătățit, fie ca sistem deschis, cu numeroase subseturi **(microkernel)** lucrând în **mod privilegiat** (*kernel mode*), cu alocare necondiționată de memorie, și cu alte module care pot lucra în **mod de utilizator** (*user mode*), neprivilegiat.

În prezent, se utilizează **sisteme de operare modulare, bazate pe microkernel-uri,** care au avantaje incontestabile față de cele monolitice în ceea ce privește posibilitățile de expandare, portabilitatea și siguranța funcționării.

O caracteristică avantajoasă a unor sisteme de operare este independența lor de tipul de hardware folosit. De exemplu, Windows NT poate fi utilizat în sisteme Intel, DEC, PowerPC ș.a.

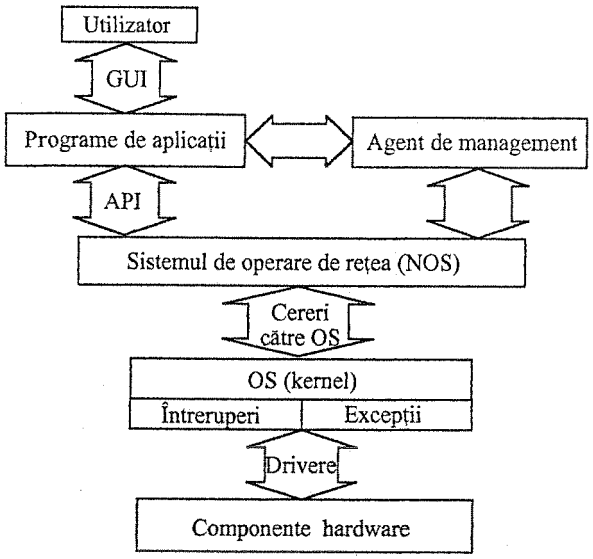


Fig. V.1 Arhitectura sistemului de tip client

Unele sisteme cu microkernel-uri pot fi concepute astfel încât să permită rularea unor aplicații realizate și cu alte kernel-uri, fiind denumite **sisteme de operare cu personalitate multiplă** (*Multiple Personality OS/ Multiple Workplace Environments*). Astfel, Windows NT permite rularea unor aplicații concepute în sisteme OS/2, Windows pe 16 sau 32 de biți.

V.2 TIPURI DE SISTEME DE OPERARE

Orice sistem de operare funcționează pe baza unor **subrutine** (*thread*) cu instrucțiuni specifice executabile la nivelul procesorului, îndeplinind **sarcini** specifice (*task*) care necesită alocarea unor resurse ale sistemului. Relația sarcină-subrutină este echivalentă cu cea părinte-copil, subrutina neavând dreptul să solicite resurse de sistem pentru execuție.

O aplicație software cu mai multe subrutine (*multithreaded*), odată lansată în execuție, reprezintă o sarcină pentru sistemul hardware. Sarcina respectivă interacționează direct cu sistemul de operare pentru a i se aloca resurse în vederea execuției. Este posibil ca o sarcină să nu poată fi executată imediat, fiind trecută într-o "coadă de așteptare" (*queue*). Aceasta este un **port logic**, în timp ce la nivelul echipamentelor, căile de intrare-ieșire reprezintă **porturi fizice.**

În sistemele hardware cu mai multe procesoare, se folosesc **sisteme de operare client** care admit **procesarea multiplă** (*Multiprocessing OS*), adică execuția diferitelor sarcini simultan, în paralel pe toate procesoarele.

Sistemele de operare care permit ca mai mulți utilizatori să folosească sistemul simultan și să ruleze diferite aplicații în același timp se numesc **sisteme de operare cu utilizatori multipli** (*Multiuser OS*).

Un sistem de operare care poate rula mai multe programe de aplicații simultan este denumit **sistem de operare cu sarcini multiple** (*Multitasking OS*).

Există două categorii de sisteme de operare care admit execuția sarcinilor multiple:

1. **sisteme cooperative** (*Cooperative Multitasking*) în care se alocă unei sarcini toate resursele, celelalte sarcini fiind în așteptare, existând riscul monopolizării sistemului;

2. **sisteme ierarhizate** (*Pre-emptive Multitasking*) care alocă resursele fiecărei sarcini lansate în execuție în funcție de prioritatea acesteia. Un criteriu de stabilire a ierarhiilor de priorități poate fi cel al timpului alocat. În momentul expirării timpului maxim de rulare a unei sarcini, aceasta este trecută în starea de așteptare și se alocă resurse altei sarcini.

MS-DOS (*Microsoft Disk Operating System*) a fost inițial proiectat ca sistem de operare cu un singur utilizator, dar în versiunile ulterioare a devenit sistem cu utilizatori multipli.

Acest sistem se instalează pe partiții formatate FAT (*File Allocation Table*), pe 16 sau 32 de biți.

DOS a fost conceput ca un program de tip linie-de-comandă, fără o interfață grafică (GUI) ușor de utilizat.

S-au proiectat sisteme de operare pentru LAN bazate pe DOS (de exemplu, WINDOWS și LANtastic), cu caracteristici din ce în ce mai sofisticate.

Începând cu versiunea 5.0, DOS a permis încărcarea programelor și fișierelor de diferite tipuri, inclusiv drivere pentru componentele hardware, în afara memoriei de bază (640 KB).

Totuși pentru a funcționa ca sistem de operare complet într-o rețea bazată pe modelul client/server a fost necesară introducerea unei GUI și a funcționalităților pentru operare în rețea, prin programele MS Windows care oferă GUI iar în versiunile recente, începând cu WIN95, includ și NOS.

Windows 3.1 oferea o GUI "prietenoasă", folosea interfețe de aplicații pe 16 biți (Win16 API) și permitea execuția sarcinilor multiple în modul cooperativ. Instalarea sistemului se făcea pe partiții formatate FAT 16.

Versiunile Win9x sunt pachete software multistrat (*multilayer client software*) care includ OS, NOS și GUI. Aceste programe utilizează interfețe de aplicații pe 32 de biți (Win32c API) care

admit execuția sarcinilor multiple ierarhizate și protecția zonelor de memorie alocate diferitelor aplicații. De asemenea, este permisă rularea aplicațiilor realizate pentru versiunile anterioare de Windows, pe 16 sau 32 de biți, precum și recunoașterea automată a componentelor hardware, prin autodetecție și autoconfigurare (PnP - *Plug-n-Play*). Instalarea sistemului se face pe partiții formatate FAT 32.

Compatibilitatea cu sistemele pe 16 biți creează o relație de subordonare a sistemului de 32 de biți față de acestea. Astfel facilitățile de operare cu sarcini multiple ierarhizate sunt blocate în cazul rulării unei aplicații pe 16 biți, reducându-se astfel performanțele sistemului.

Sistemele Windows NT, Windows 2000, Windows XP , cu versiuni diferite ca preț și complexitate pentru servere și utilizatori particulari (*home users*), oferă facilități sporite privind securitatea și siguranța sistemului.

Win2k poate fi instalat atât pe partiții FAT32 cât și NTFS (NT *File System*).

WinNT și WinXP rulează numai pe partiții non-DOS, formatate NTFS, ceea ce face imposibilă rularea aplicațiilor definite exclusiv sub DOS.

WinNT utilizează diferite interfețe de aplicație pe 32 de biți, cu diverse caracteristici:

- Win32 API cu facilități de operare numai pe 32 de biți, definită numai pentru aplicații create sub Windows NT;
- Win32s API reprezintând un **subset** de interfețe pe 32 de biți, provenite din Win16 API. Acestea sunt definite într-o bibliotecă dinamică (DLL - *Dynamic Link Library*) și permit rularea aplicațiilor pe 16 biți create pentru Win3.1, prin conversia cererilor pe 32 de biți în formatul Win16;
- Win32c API, **compatibile** cu Win16 API, prezintă aproape toate facilitățile interfețelor originale pentru WinNT. Sunt utilizate pentru rularea aplicațiilor create pentru Win9x sub WinNT.

Windows NT introduce o facilitate suplimentară față de sistemele Win9x și anume **procedura de apel local** (LPC - *Local Procedure Call*) prin intermediul căreia se alocă, la cerere, resurse hardware tuturor aplicațiilor. Astfel aplicațiile nu mai comunică direct cu sistemul, ceea ce face ca anumite programe, de exemplu jocurile, definite pentru versiunile anterioare de Windows, să nu mai poată fi rulate cu performanțe optime sub WinNT.

Programele de aplicații (Win32 *client*) și subsistemele de securitate lucrează sub WinNT în modul neprivilegiat. Subsistemele de management și kernelul lucrează în mod privilegiat, cu acces direct la resursele hardware ale sistemului.

Rularea sub WinNT a aplicațiilor create pentru alte sisteme de operare (OS/2, Win16) se realizează în subsisteme dedicate acestora, denumite **mașini virtuale** (*virtual machine*), WinNT fiind un sistem cu personalitate multiplă.

Un alt sistem de operare foarte apreciat de utilizatori este sistemul **UNIX**, definit în diferite variante: BSD-UX (*Berkeley Software Distribution Unix*), SVR4-UX (*At&T System V Release 4 Unix*), HP-UX (*Hewlett-Packard Unix*), Ultrix (dezvoltat de DEC), Solaris (definit de Sun Microsystems), Open Server (definit de SCO - *Santa Cruz Operation*) etc.

Indiferent de firma producătoare, Unix este un OS cu utilizatori multipli, care suportă procesarea multiplă simetrică, execuția ierarhică a sarcinilor multiple, rularea simultană a mai multor subrutine și admite modurile de utilizator, neprivilegiat, și kernel, privilegiat, pentru protecția resurselor hardware ale sistemului (*kernel-based, multiuser, multiprocessing, multitasking, multithreaded OS*).

Ca și DOS, Unix este un program de tip linie-de-comandă, criptic, recomandat îndeosebi mediilor științifice.

Novell DOS versiunea 7 (ND7) este un pachet de programe care include DOS (echivalent MS DOS 6.22), precum și sistemul de operare în rețea (NOS) pentru clienții NetWare cu programe de servicii (e-mail, chat etc) specifice. Ca avantaje ale ND7 se evidențiază faptul că acest sistem de operare (*multitasking kernel*) poate rula aplicații Windows, permite crearea rezervelor de sistem (*backup*), detecția virușilor și managementul rețelei.

OS/2 este un sistem de operare similar cu WinNT dar incompatibil cu acesta, care include mașini virtuale implementate distinct pentru aplicații proiectate pentru OS/2, DOS sau Windows pe 16 sau 32 de biți.

V.3 MODELUL STRUCTURAT AL UNUI SISTEM DE OPERARE DE REȚEA

Comunicația dintre un calculator și rețea se realizează fizic prin intermediul plăcii de rețea iar logic (*software*) prin sistemul de operare de rețea (NOS).

Comunicația dintre programele de aplicație și NOS se realizează prin intermediul unei interfețe de aplicații (API). Pentru rețele de PC-uri interfața API standard este **NetBIOS API** (*Network Basic Input Output System API*).

NetBIOS este prin definiție un sistem de comenzi care realizează:

- interpretarea cererilor adresate NOS de către programele de aplicații;
- transferul acestor cereri către programul de comunicație cu rețeaua.

Utilizatorul unui calculator-client din rețea poate solicita un serviciu care implică fie resurse locale, fie resurse din rețea, de pe un server sau alt calculator-client.

Protocolul NetBIOS de redirecționare (NetBIOS *Redirector*) transferă cererea în format NCB (*Network Control Block*) fie sistemului de operare local, fie către NetBIOS API care o convertește în formatul acceptat de rețea (SMB - *Server Message Block*), o trimite către NOS iar acesta o comunică plăcii de rețea în vederea transferului în LAN. Serverul răspunde cererii clientului pe baza **protocolului SMB** definit în NetBIOS.

Orice NOS poate fi structurat pe baza modelului OSI.

Pe nivelele inferioare OSI 1 și 2, orice NOS poate lucra pe baza oricărui standard de LAN.

Diferențierile între diverse NOS apar abia pe nivelele OSI superioare, în funcție de protocoalele implementate de fiecare (Fig. V.2).

Comunicația client-server este posibilă numai dacă se folosește același protocol de transport. De aceea, în multe sistem de operare sunt incluse mai multe protocoale de transport.

În general, TCP/IP este considerată stivă de protocoale universală și este inclusă în majoritatea sistemelor de operare de rețea, pentru clienți și servere.

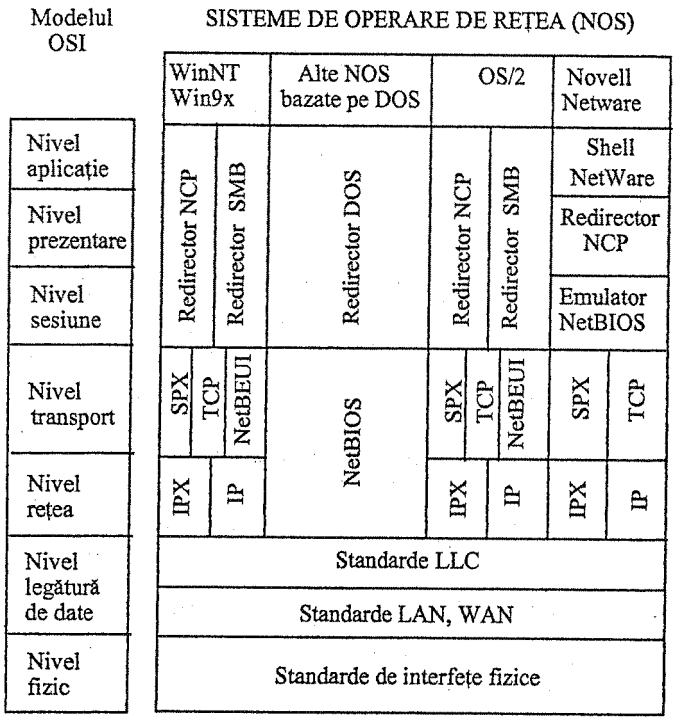


Fig.V.2 Protocoalele implementate în diferite NOS

Observații:

1. Pentru alte NOS, interfețele pentru programele de aplicații (API) sunt denumite:

- **socluri** (*socket*) pentru Berkeley Unix;
- SPX/IPX pentru rețele Novell NetWare.

2. Se folosesc trei tipuri de **interfețe de utilizator**:

- interfețe bazate pe caractere, pentru programele de tip 'linie-de-comnadă';
- interfețe grafice de utilizator (GUI), orientate pe obiect;
- interfețe sociale, care se doresc a fi mult mai dinamice decât cele grafice, mai bine adaptate capacităților de lucru ale utilizatorului, 'simțind' când acesta are nevoie de ajutor și oferindu-i sugestii fie prin intermediul unor meniuri de tip HELP, fie direct pe ecran, prin scurte comentarii.

În prezent, toate firmele producătoare de software dezvoltă astfel de interfețe. Prima interfață socială dezvoltată de Microsoft se numește BOB. Pentru Windows 9x se folosește interfața **Simply Village,** fiind similară în multe aspecte cu sistemul de indicatoare amplasate într-o localitate.

3. Pentru Unix se folosește o interfață grafică cu ferestre multiple (*X Windows*), proiectată pentru mai multe platforme Unix (HP, IBM, Sun, Novell) cunoscută sub abrevierea CDE (*Common Desktop Environment*).

4. WinNT și Unix nu sunt incompatibile. De exemplu, pachetul *eXceed 4 Windows NT* permite sistemului NT să lucreze ca un server X (Unix) pentru clienții X și, în același timp, să ruleze aplicații sub Windows pentru clienții Windows. În general, se folosește un program sau un modul hardware de emulare care implementează **protocolul de prezentare a ferestrelor X** (*X Windows Presentation Protocol*) pentru schimbarea formatului datelor dintr-o interfață în alta. Totuși trebuie apreciată corect necesitatea utilizării mai multor platforme în aceeași rețea.

5. Pentru a permite furnizarea de servicii în bune condiții în rețea, sistemele de operare pentru servere includ funcții suplimentare celor oferite clienților, mai precis module software dedicate:

- securizării transmisiei;
- autentificării mesajelor;
- criptării datelor;
- gestionării resurselor hardware ale calculatorului-server, având capacitate mare de stocare a informațiilor, memorii RAM rapide, placă de rețea multiport, eventual mai multe procesoare.

V.4 TIPURI DE DRIVERE PENTRU PLĂCILE DE REȚEA

Întrucât majoritatea sistemelor de operare în rețea (NOS) implementează protocoale multiple, respectiv mai multe suite de protocoale (TCP/IP; IPX/SPX), este necesar ca driverele plăcilor de rețea să fie compatibile cu acestea.

Inițial firmele producătoare de cartele de rețea au creat drivere monolitice, pentru o suită unică de protocoale. De exemplu, firma Novell a dezvoltat drivere pentru suita IPX/SPX, care constau într-un fișier unic IPX.com, asociat fișierului IPX.obj printr-un proces logic wsgen.

Driverele unice au avantajul că pot fi ușor create și îmbunătățite (*up-date*), dar sunt incompatibile cu alte suite de protocoale.

Ulterior industria de software a adoptat o nouă politică de proiectare a driverelor NIC care trebuie să suporte protocoale multiple. Această tendință este valabilă și pentru driverele altor tipuri de echipamente de rețea.

Firmele Microsoft și 3Com au elaborat în colaborare standardul pentru driverele plăcilor de rețea NDIS (*Network Driver Interface Specification*).

Firmele Novell și Apple au propus dezvoltarea **interfețelor deschise pentru legăturile de date** (*ODI - Open Data-link Interface*).

În prezent, majoritatea driverelor de NIC suportă protocoale multiple, incluzând specificațiile NDIS, cât și cele ODI.

Un driver NDIS stabilește comenzile standard pentru comunicația dintre un NOS, cu diferite suite de protocoale, și NIC, cu driverul asociat (NDIS MAC *Driver*). Gestionarea acestui proces de comunicație se face prin programul de management de protocol.

Specificațiile NDIS stabilesc faptul că la pornirea unui calculator bazat pe DOS, se execută fișierul Config.sys prin care se lansează programul de management. Acesta accesează fișierul de tip text protocol.ini pe baza căruia se inițializează driverele componentelor, inclusiv cele de protocol și NIC, stabilind legăturile dintre acestea (*binding*),după care creează o imagine a acestui fișier în memorie.

Orice nou driver instalat va fi comparat cu parametrii de configurare existenți și adăugat la fișierul protocol.ini de către agentul de management.

După stabilirea configurației corecte, se fac legăturile cu protocoalele de nivel superior prin intermediul subnivelului **vector,** inclus în nivelul legătură de date (Fig. V.3) și se salvează configurația în fișierul protocol.ini.

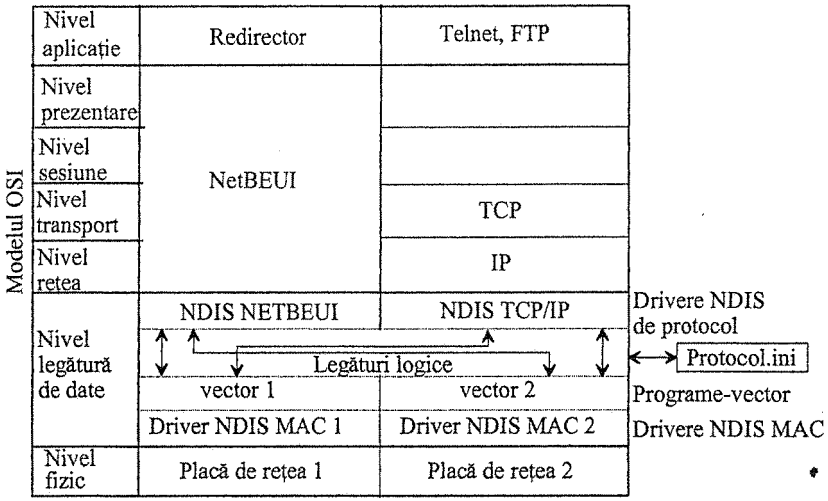


Fig. V.3 Arhitectura NDIS

Conform **specificațiilor ODI,** informațiile de configurare referitoare la drivere și protocoalele implementate în NOS sunt stocate în fișierul net.cfg, fiind gestionate de programul LSL.com corespunzător subnivelului LSL (*Link Support Layer*), din cadrul nivelului OSI legătură de date (Fig. V.4).

Conform ODI, driverele plăcilor de rețea se numesc **drivere pentru interfețe cu legături multiple** (MLID - *MultiLink Interface Driver*). Orice driver MLID comunică prin intermediul unei interfețe cu legături multiple cu subnivelul de suport a legăturii care la rândul său comunică prin intermediul interfeței multiprotocol cu orice suită de protocoale de pe nivelele OSI superioare.

Driverele plăcilor de rețea pentru magistrale PCMCIA (PC *cards*) includ interfețele cu sistemul de operare local (OS) și cu cel de rețea (NOS) implementate pe baza specificațiilor NDIS și ODI, precum și interfața cu controlerul PCMCIA, realizată conform **specificațiilor CSS** (*Card and Socket Specification*), care prevăd două subnivele logice:

- subnivelul CS (*Card Services*), independent de caracteristicile hardware, realizează interfațarea cu OS și NOS, fiind responsabil de transmiterea mesajelor de eroare, de gestionarea resurselor și de configurarea plăcii de rețea;
- subnivelul SS (*Socket Services*), dependent de partea hardware și evident de firma producătoare, furnizează informațiile referitoare la introducerea și extragerea 'la cald', în timpul funcționării, a cartelei de rețea din portul fizic (*hot-swapability*), fără a fi necesară reconfigurarea lor.

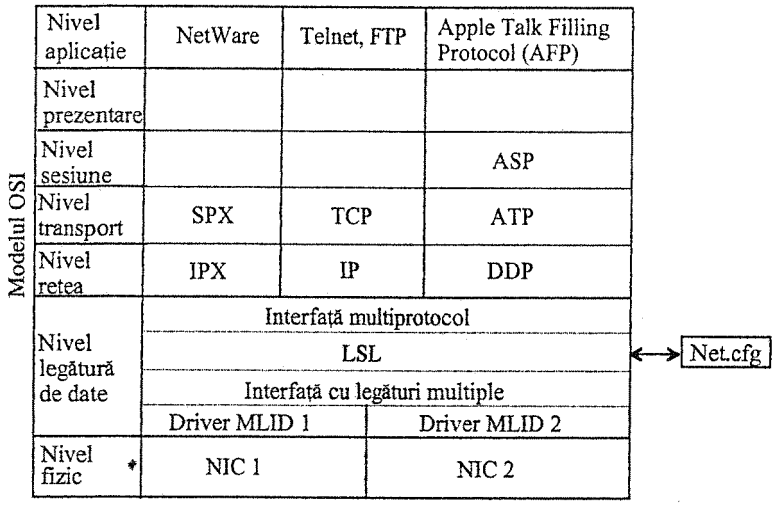


Fig. V.4 Arhitectura ODI

Observații:

1. Majoritatea echipamentelor de comunicații se achiziționează cu un set extins de drivere proiectate pentru diverse sisteme de operare. De asemenea, sistemele de operare au incluse arhive cu driverele pentru echipamentele diferitelor firme astfel încât în cazul celor PnP se încarcă automat driverul corespunzător.

2. În afara standardelor aminitite mai-sus, există standarde și pentru driverele plăcilor de rețea utilizate în alte rețele (ATM, ISDN etc).

3. Calculatoarele-server pot fi dotate cu **plăci de rețea multiple** sau **multiport**, compatibile cu mai multe suite de protocoale (MNP - *Multiple Network Protocol*). Se pune problema în acest caz ca sistemul de operare în rețea instalat pe server să poată lucra simultan cu diversele suite de protocoale, adică să admită, pe principiul sistemelor deschise, comunicația simultană cu clienți având sisteme de operare de rețea distincte. În acest caz, serverul devine **router multiprotocol** sau **poartă de rețea** (*gateway*).

4. Windows NT nu admite comunicația directă dintre aplicații și componentele hardware prin intermediul driverelor clasice care operează în mod real (*real-mode driver*). Prin introducerea interfețelor de aplicație (API) pentru comunicația cu sistemul de operare și a procedurii de apel local (LPC) ca subnivel de control al accesului spre nivelul fizic, sistemul devine extrem de stabil iar driverele folosite apar ca **drivere virtuale** (VxD - *Virtual Device Driver*) față de sistemul de operare.

V.5 WINDOWS NT

Windows NT este un sistem de operare **multistrat** scris în limbajul C, incluzând OS, NOS și GUI, **portabil** în sensul că poate fi executat cu diverse procesoare produse de diferite firme (Intel, AMD, RISC, DEC Alpha etc) și **scalabil** întrucât suportă procesarea multiplă simetrică (SMP - *Symmetric Multiprocessing*). Totodată, WinNT admite accesul simultan al mai multor utilizatori (*multiuser*), rularea în paralel a mai multor aplicații (*preemptive multitasking*), a mai multor subrutine (*multithreading*), fiind un sistem stabil, sigur, cu capacități de procesare deosebite referitor la operații complexe de gestionare a bazelor de date, a sistemului de fișiere și a altor servicii.

Arhitectura sistemului WinNT (fig.V.5) include **executorul NT** (NT *Executive*), lucrând în modul kernel, și setul de **aplicații de tip client/server**, care se execută în modul de utilizator.

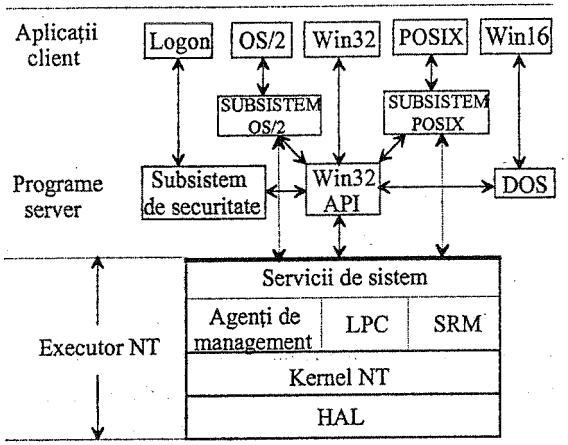


Fig. V.5 Arhitectura sistemului Windows NT

Executorul NT include kernelul NT și subsistemele de servicii de sistem:

- agenții de gestionare a obiectelor, proceselor, memoriei virtuale și sistemului de intrări-ieșiri (incluzând driverele pentru memoria cache, sistemul de fișiere și alte componente);
- procedura de apel local (LPC - *Local Procedure Call*);
- subsistemul de monitorizare a securității (SRM - *Security Reference Monitor*).

Un rol important în creșterea performanțelor Windows-ului NT față de alte OS îl are sistemul de management al memoriei cache, care minimizează numărul de operații de citire/scriere din și în memorie.

Pentru a permite aplicațiilor să ruleze cu o capacitate mai mare de memorie decât cea instalată, WinNT poate aloca, prin intermediul sistemului de gestiune a memoriei virtuale, zone de memorie de pe HDD (*swap memory*) de până la 4GB pentru fiecare aplicație. WinNT protejează zonele de memorie alocate diverselor aplicații.

WinNT suportă diverse sisteme de fișiere, cu drivere specifice:

- NTFS - exclusiv pentru aplicații NT;
- FAT - numai pentru diskete;
- CDFS (*Compact Disk File System*) - pentru CD-uri;
- HPFS (*High-Performance File System*) - pentru aplicații OS/2.

Windows NT folosește pentru fiecare fișier spre sistemul de fișiere adecvat.

Sistemul FAT creat pentru DOS utilizează convenția 8.3 pentru numele de fișiere.

În format NTFS, lungimea maximă a numelor de fișiere este de 255 de caractere. De aceea, transferul fișierelor din sistem NTFS în sistem FAT/DOS impune conversia formatului numelui (de exemplu, un fișier denumit abcdefghij.doc va fi numit pe partiția FAT: abcdef~1.doc). Pot fi create partiții FAT și NTFS pe același HDD. Sistemul FAT pentru Windows NT admite stocarea fișierelor pe diskete cu nume de lungime maximă de 255 de caractere.

HPFS suportă nume de fișiere cu cel mult 255 de caractere, folosește o structură de directoare în formă de 'arbore' și minimizează fragmentarea fișierelor stocate pe HDD.

NTFS preia atributele sistemelor FAT și HPFS dar introduce și caracteristici noi:

- controlul accesului se poate face atât la nivel de director, cât și la nivelul fișierelor;
- utilizează tabele 'master' de fișiere (MFT - *Master File Table*), cu caracter redundant față de NTFS, în care sunt stocate atributele tuturor fișierelor iar fișierele de mici dimensiuni (sub 1500 de octeți) sunt în întregime stocate în MFT;
- admite compatibilitatea cu sistemul POSIX pentru UNIX prin respectarea caracteristicilor fișierelor create în UNIX: diferențierea literelor mari de cele mici (*case-sensitive*), stabilirea atributelor temporale de creere și accesare a fișierelor etc.
- permite detecția sectoarelor de disc defecte (*bad sectors*), marcarea lor automată și mutarea fișierelor în alte zone ale memoriei, fără intervenția utilizatorului;
- refacerea rapidă a sistemului de operare în cazul unei funcționări neadecvate.

Kernelul NT, prin mecanismul de întreruperi și excepții, realizează transferul mesajelor dintre sistemul de operare și partea hardware, prin intermediul **nivelului de abstractizare fizică**

(HAL - *Hardware Abstraction Layer*), echivalent sistemului BIOS utilizat de DOS. Refacerea sistemului și securizarea cad de asemenea în sarcina kernelului NT.

Pe nivelul superior, apar procese de comunicație între **aplicațiile-client** și cele de tip **server**:

- procesul de accesare a sistemului de către un utilizator NT (*logon process*) și subsistemul de securitate;
- aplicații proiectate pentru alte sisteme de operare (OS/2, Win32, Win16, Posix) și interfețele de aplicații specifice.

Portabilitatea Windows-ului NT se realizează prin compilarea codului-sursă cu ajutorul compilatoarelor C din fiecare sistem, compatibile între ele, în vederea execuției cu diverse procesoare având nivele HAL adaptate acestora.

Tot în limbaj C sunt scrise și driverele pentru componentele hardware (mouse, tastatură, imprimantă etc) și cele pentru protocoalele de comunicație în rețea (NetBIOS, redirectoare NCP și SMB, TCP/IP, NetBEUI, IPX/SPX). Specificațiile NDIS pentru driverele plăcilor de rețea simple și multiport prevăd posibilitatea utilizării protocoalelor multiple.

Accesul rapid la fișiere și **siguranța** de funcționare (*reliability*) a sistemului WinNT sunt date de redundanța tabelelor de fișiere MFT, primar și secundar sau 'oglindă' (*MFT Mirror*), stocate în sectorul de BOOT primar, respectiv în sectorul de BOOT de rezervă (*Duplicate BOOT Sector*).

Un avantaj major al NTFS este dat de rapiditatea de refacere a sistemului de fișiere (*File System Recoverability*) în cazul unor defecte majore (*Crash*). Orice tranzacție cu fișiere este monitorizată și periodic se notează starea acesteia, în așa-numitele 'puncte de verificare' (*checkpoints*). În cazul distrugerii sistemului de fișiere, NTFS reia tranzacțiile din aceste puncte, fie continuându-le, fie anulând efectele acestora (*undo*), astfel ca starea finală a sistemului să fie corectă, fără erori. Recuperarea NTFS se face în doar câteva secunde.

V.5.1 Domenii NT

Informațiile despre utilizatorii și resursele sistemului WinNT nu sunt incluse într-o bază de date unică, ci în mai multe baze de date distribuite în rețea, guvernate însă de un singur sistem de securitate, pentru autorizarea accesului din orice nod al rețelei.

Rețelele NT sunt structurate pe **domenii** incluzând mai multe servere Windows NT subordonate subsistemului de securitate care controlează accesul la un domeniu.

Informațiile referitoare la fiecare domeniu sunt stocate pe serverul NT care oferă **serviciile de domeniu.**

Un singur server din rețeaua NT devine **controlerul primar al domeniului** (*Active/Primary Domain Controller*). Celelalte servere din domeniu pot să reprezinte doar rezerve ale acestuia sau să aibă cu totul alte funcții (servere de aplicații; servere care oferă servicii de rețea etc).

Calculatoarele de tip client WinNT pot forma **grupuri de lucru** (*workgroups*) care diferă de domeniile NT prin aceea că nu dispun de un sistem unic de securitate, fiecare calculator fiind responsabil de aplicarea politicilor de securitate la nivelul său.

Într-un domeniu oricare controler, primar sau secundar, poate autoriza accesul unui utilizator în rețea, în timp ce în grupurile de lucru, pe fiecare calculator se stabilesc și se păstrează **listele de control al accesului** (ACL - *Access Control List*), cu conturile de utilizator create pentru acea stație.

Într-o rețea NT, alcătuită din mai multe domenii, trebuie stabilit modul de autorizare a accesului dintr-un domeniu în altul, pentru realizarea comunicației între domenii, pe baza unor **relații de încredere:**

1. **exclusivă** (*Trust Relationship*), numai între două domenii, pe baza procedeului de extindere a autentificării (*passthrough authentication*) dintr-un domeniu într-altul, astfel încât un utilizator admis într-un domeniu poate accesa și resursele celuilalt domeniu. Aceste relații sunt restrictive în cazul a trei sau mai multe domenii întrucât dacă între domeniile A și B s-a stabilit o relație de încredere exclusivă, și similar între domeniile B și C, aceasta nu permite utilizatorilor din domeniul A să acceseze resursele domeniului C.

2. **totală** (*Interdomain trust accounts*), între toate domeniile definite în rețea. În acest caz, un controler de domeniu poate permite accesul unui utilizator în oricare alt domeniu.

3. **între stații și servere** (*Workstation trust accounts*), astfel ca autentificarea în vederea accesului într-un domeniu, să se poată realiza și la nivelul stației, fără intervenția serverului cu rol de controler de domeniu.

4. **între servere** (*Server trust accounts*), pe baza acestora realizându-se copiile de siguranță ale bazelor de date stocate pe controlerul primar de domeniu pe serverele secundare (*Backup Domain Controller*).

Arhitectura rețelei NT poate fi proiectată folosind diverse **modele de domenii** (Fig.V.6):

- **domeniul unic** - această arhitectură admite cel mult 10 000 de utilizatori și un singur sistem de securitate (SAM - *Security Account Manager*).
- **domeniile multiple independente** - resursele domeniilor sunt total separate și protejate, gestionate independent, între domenii nefiind stabilite relații de încredere.
- **domeniul "master" unic** - permite implementarea ierarhică a rețelei NT, cu un domeniu principal (*master*) și mai multe domenii subordonate. Conturile de utilizator (maxim 10 000) sunt

definite în domeniul principal și gestionarea resurselor se face centralizat, cu un singur agent de management. Accesul din domeniul master în domeniile subordonate este permis pe baza relațiilor de încredere dar nu este admis accesul dinspre subdomenii în domeniul principal.

- **domenii "master" multiple** - această arhitectură extinsă admite până la 10 000 de utilizatori pentru fiecare domeniu master, care deține încrederea domeniilor subordonate lui.
- **domeniile multiple dependente** - reprezintă o arhitectură ideală, cu relații de încredere totală stabilite între oricare două domenii.

În funcție de natura activităților desfășurate în rețea, se alege arhitectura NT potrivită.

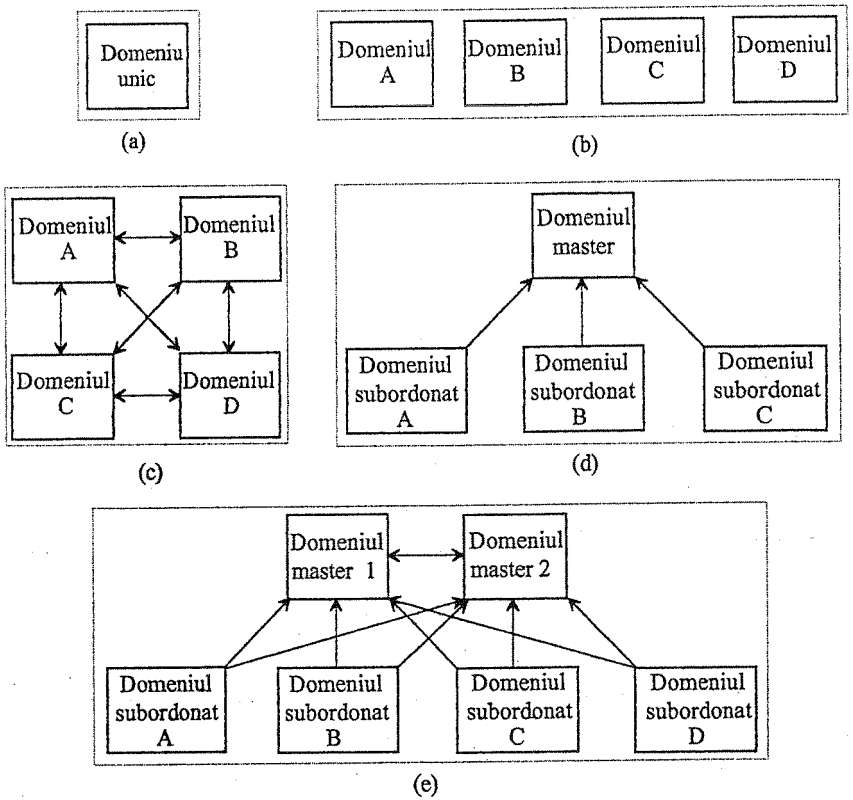


Fig. V.6 Arhitecturi NT: (a) cu domeniu unic;
(b) cu domenii multiple independente;
(c) cu domenii multiple dependente;
(d) cu domeniu master unic;
(e) cu mai multe domenii master.

V.5.2 Servicii NT

Windows NT furnizează diverse servicii de rețea, pe baza unei arhitecturi de protocoale stratificate conform modelului de rețea OSI (Fig. V.7).

Placa de rețea cu driver de tip NDIS poate comunica cu mai multe suite de protocoale: TCP/IP, IPX/SPX, NetBEUI, AppleTalk, DLC (*Data Link Control*).

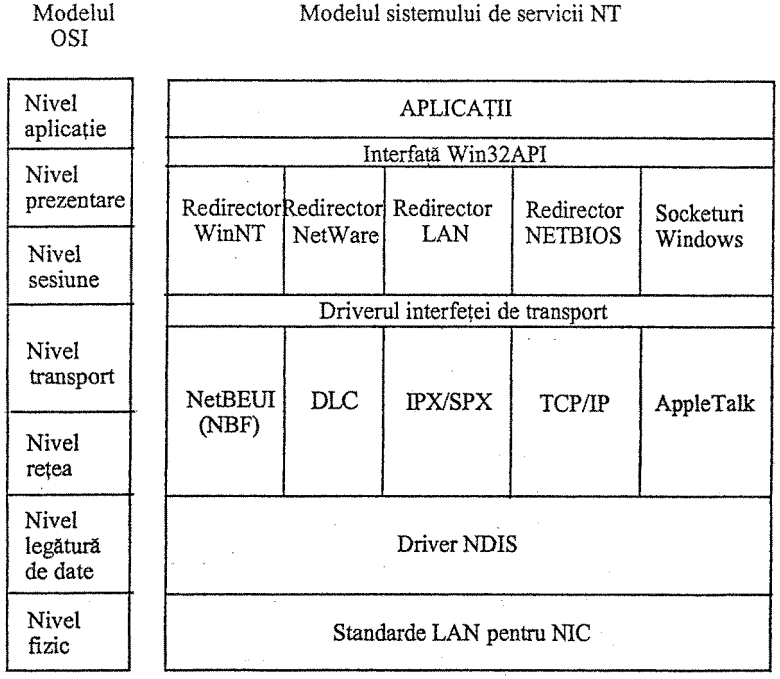


Fig.V.7 Sistemul serviciilor de rețea NT

Pe baza modelului client/server, Windows NT poate lucra simultan cu protocoale definite pentru diverse NOS:

- NBF (NetBEUI *Frame*) este versiunea NT a NetBEUI pentru sisteme OS/2 și Microsoft LAN Manager;
- DLC pentru comunicația cu imprimante de rețea (de exemplu, Hewlett-Packard LaserJet), calculatoare de tip "mainframe" IBM și servere-gateway Microsoft SNA (*Service Network Architecture*) pentru Windows NT;

- IPX/SPX sau NWLink pentru clienți și servere NetWare;
- TCP/IP pentru rețele de PC-uri bazate pe WinNT, cu facilități de configurare pentru DHCP și servere WINS;
- AppleTalk pentru clienți și servere Macintosh.

Interfața de transport asigură transparența comunicării între diversele protocoale de transport și redirectoarele admise de WinNT, cu diferite **opțiuni de comunicare între procese**:

- **WinSock** (rulat din fișierul WinSock.DLL) este cel mai flexibil mecanism de comunicare interprocese pentru aplicații distribuite între clienți și servere sub Windows NT. Versiunea WinSock2 are suport multiprotocol (IPX/SPX, AppleTalk, DECnet, OSI) și lucrează cu două interfețe, una pentru aplicații, WinSock API, și alta pentru selectarea protocolului de transport, WinSock SPI (*Service Provider Interface*).
- **NetBIOS** este interfața API (implementată în fișierul NetBIOS.DLL) pentru comunicații între procese, în cazul aplicațiilor distribuite, cu redirector NetBIOS și suita de protocoale NBF. Mesajele dintre clienți și servere se realizează în format SMB.
- **RPC** (*Remote Procedure Call*) este un mecanism superior de comunicare între procese, definit de DCE (*Distributed Computing Environment*), pentru rularea aplicațiilor distribuite în rețea, pe mai multe calculatoare. RPC poate utiliza pentru anumite aplicații interfețele WinSock și NetBIOS. Serviciul RPC este oferit de modulul RPC inclus în sistemul de operare.

Pentru compatibilitatea cu sistemul OS/2, Windows NT include și alte mecanisme de comunicare între procese (*Named Pipes, Mail Slot*).

Comunicațiile între procese, indiferent de tipul de interfață utilizat, se pot face fie în mod sincron, orientat pe conexiune, fie asincron fără conexiune.

Orice comunicație între procese se realizează cu permisiunea sistemului de securitate NT, care pe de o parte autorizează accesul utilizatorilor la resursele locale și de rețea, în funcție de drepturile acordate fiecăruia în mod diferențiat, și pe de altă parte supervizează schimburile de informații dintre procese pentru a nu se încălca în nici un fel politica de securitate.

Windows NT folosește un sistem de monitorizare a aplicării regulilor de securitate (SRM), care lucrează în modul kernel. Acesta urmărește respectarea nivelelor de acces ale utilizatorilor, cu diverse permisiuni: de citire, scriere sau ștergere de fișiere, execuție de programe, schimbarea drepturilor sau crearea conturilor de utilizator, interzicerea parțială sau totală a accesului la resursele sistemului. Conturile de utilizator și parametrii de configurare a acestora sunt stocate într-o bază de date care se păstrează în controlerul primar de domeniu. Copii ale acesteia pot exista pe serverele NT de backup.

Observații:

1. Interoperabilitatea dintre Windows NT și alte sisteme de operare implică soluționarea problemelor de compatibilitate pe toate nivelele modelului OSI. La nivele inferioare, această problemă este soluționată pe baza standardelor pentru plăcile de rețea și driverele acestora, specificațiile NDIS și ODI permițând utilizarea mai multor suite de protocoale pe nivelele de rețea și de transport. Pe nivelele OSI superioare, în funcție de sistemul de fișiere utilizat de client și de server (NTFS, NetWare etc), compatibilitatea poate fi realizată fie direct cu redirectoare NCP sau SMB care stabilesc formatul acceptat pentru comunicația între procese, fie indirect cu module software (*shell*) Netware create special pentru acest tip de rețea, redirector NCP și emulator NetBIOS pentru conversia de format. În cazul comunicației NT/Unix, standardul X Windows face posibilă comunicația client-server având sisteme de operare distincte, folosind protocolul Telnet.

2. Accesul de la distanță într-un sistem NT (RAS - *Remote Access Service*) reprezintă un serviciu NT furnizat prin module software specializate, de tip client și de tip server.

Modulul RAS server se execută pe serverul NT și este responsabil de **autentificarea** accesului de la distanță a utilizatorului, eventual cu parolă criptată (*encrypted authentication*), și supravegherea sesiunilor de comunicație create de acesta. Acest modul permite maximum 256 de conexiuni simultane stabilite de la distanță. Protocoalele de autentificare utilizate de RAS sunt:

- CHAP (*Challenge Handshake Authentication Protocol*) cel mai sigur protocol, care criptează atât parola cât și datele transmise într-o sesiune.
- SPAP (*Shiva Password Authentication Protocol*) criptează numai parola de acces a utilizatorului, fiind obligatorie aplicarea lui atât la client cât și pe server.
- PAP (*Password Authentication Protocol*) autorizează accesul pe baza unei parole de utilizator, transmisă necodat (*clear-text*).

Accesul la serverul NT se poate face fie printr-o legătură telefonică (*dial-up*), fie în sistem ISDN sau X.25.

Modulul RAS client poate opera sub DOS, Windows NT precum și alte versiuni Windows, cu diferite suite de protocoale (TCP/IP, IPX/SPX, NBF) și diverse protocoale pe nivelul legătură de date (NDIS, PPP).

V.6 UNIX

UNIX este un sistem de operare modular, structurat pe două nivele (Fig.V.8):

1. **kernelul** UNIX include modulele de gestionare a resurselor (CPU, HDD, memorie instalată, memorie virtuală), sistemul de fișiere, driverele de componente, modulul de securitate,

sistemul de intrări/ieșiri (I/O - *Input/Output*), modulul de control a proceselor, sistemul de întreruperi;

2. **programele** de sistem UNIX pot fi: compilatoare, interpretoare, aplicații, programe utilitare, biblioteci de program, procese ale utilizatorului (*shell*).

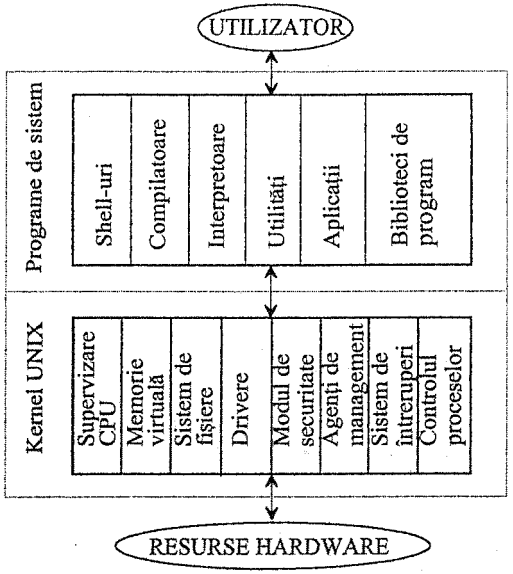


Fig.V.8 Arhitectura sistemului de operare UNIX

Sistemul UNIX nu conține modulele software pentru comunicația în rețea, pentru aceasta fiind utilizată suita de protocoale TCP/IP combinată cu sistemul de fișiere în rețea NFS (*Network File System*), împreună alcătuind sistemul de operare de rețea NOS (Fig. V.9).

S-au dezvoltat diferite variante de UNIX, în diverse limbaje de programare (în principal, C), implementate pentru diferite sisteme hardware, în prezent fiind dezvoltat un standard unic (*Spec 1170 APIs*), reprezentând o colecție de peste 1000 de interfețe de aplicații (API), care poate să suporte toate versiunile UNIX. În paralel, s-a proiectat o interfață grafică de utilizator CDE unică pentru aplicațiile dezvoltate în orice sistem UNIX.

UNIX a fost conceput ca **sistem modular**, în care se pot introduce noi module software, fie în kernel, fie în grupul fișierelor de sistem.

Compilarea codului-sursă la nivelul fiecărui sistem hardware conferă UNIX-ului caracteristica de **portabilitate**, între diverse echipamente hardware precum și între diferitele versiuni de UNIX.

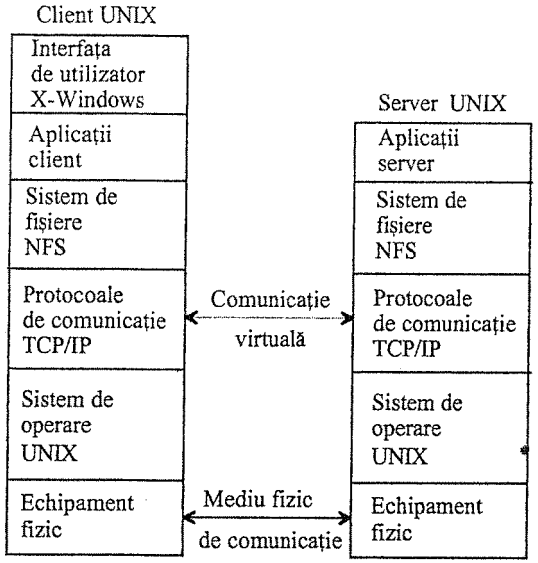


Fig.V.9 Modelele structurate ale sistemelor client și server UNIX

Aplicațiile-client sunt cele care comunică direct cu utilizatorul (*Front-End Client Application*). Cele de tip server rulează în mod transparent față de clienți (*Back-End Server Application*).

Asemenea WinNT, UNIX admite utilizatori multipli, rularea simultană a mai multor aplicații în modul ierarhic, instalarea în sistem cu mai multe procesoare (*multiuser, pre-emptive multitasking, multithreaded, multiprocessing OS*).

Accesul la un sistem UNIX se face pe baza numelui și parolei de utilizator, eventual a numelui stației dacă sistemul este accesat de la distanță (*remote access*).

Spre deosebire de alte sisteme de operare, UNIX este **dinamic** în sensul că orice utilizator poate să intervină în structura sa și să-și creeze propriile aplicații.

Pentru a crea noi aplicații UNIX, fiecare utilizator poate să scrie module software (*shell script*) în diverse limbaje de programare: C, Turbo-C, PERL (*Practical Extraction and Reporting Language*) etc. Interfața utilizatorului cu sistemul este realizată prin programele de interpretare a comenzilor.

Există mai multe tipuri de shell-uri UNIX (cu prompteri diferiți), cele mai utilizate fiind:

- Shell-uri Bourne (*bash*)
- Shell-uri C (*csh*)

- Shell-uri Korn (*ksh* - combinație între *csh* și *bash*).

Editarea acestor shelluri (*scripting*) se poate face cu diverse editoare de text pentru UNIX, de exemplu, TCL&TK. TCL (*Tool Command Language*) este un limbaj de scriere și interpretare a comenzilor, utilizat pentru realizarea comunicației între aplicații dezvoltate în diverse medii.

Sistemul de fișiere utilizat de UNIX este structurat ierarhic sub forma unui 'arbore', cu mai multe nivele și un nod 'rădăcină' (Fig.V.10). Fișierele sunt interpretate ca șiruri de octeți și sunt grupate în directoare, directorul 'rădăcină' fiind notat simplu cu caracterul '/'.

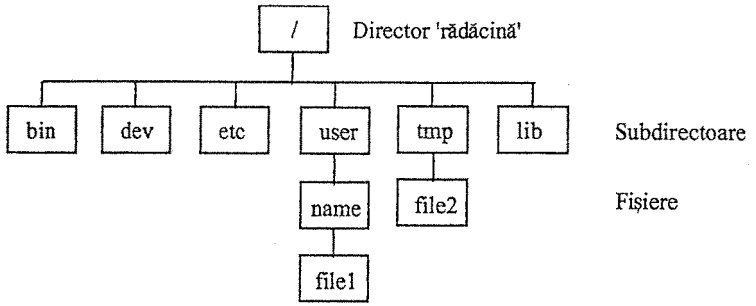


Fig.V.10 Structura sistemului de fișiere UNIX

Accesarea fișierelor și directoarelor se poate face exprimând fie calea absolută pornind din nodul 'rădăcină', fie calea relativă la un alt nod (Anexa B).

De exemplu, calea absolută care identifică fișierul file1 este: /user/name/file1 iar calea relativă la directorul curent este name/file1.

UNIX suportă existența mai multor sisteme de fișiere pe același disc, permite alocarea de memorie virtuală aplicațiilor (*swap memory*) și stocarea driverelor în afara kernelului.

Ca mecanism de comunicare între procese, UNIX folosește așa-numitele **socluri** (*socket*), asociate cu adresele zonelor de memorie alocate diverselor procese. TCP folosește socketuri de tip "șir" (*stream socket*), UDP lucrează cu socketuri de tip "datagramă" iar în cazul comunicației între două procese de pe nivele OSI diferite se implementează socketuri "brute" (*raw socket*) care trebuie să realizeze și funcțiile altor nivele OSI, necesare în procesul de comunicație.

VI

INTERCONECTAREA REȚELELOR LOCALE

Creșterea volumului de date vehiculate în rețelele de arie largă, în particular în Internet și WWW, impune utilizarea unei lățimi de bandă tot mai mari și a unor sisteme de operare mai rapide (Windows, Unix, Mac), care admit efectuarea simultană a mai multor sarcini (*multitasking*), deci și a tranzacțiilor multiple, simultane cu rețeaua.

Creșterea lățimii de bandă disponibile pentru utilizatorii unei rețele locale, este posibilă prin **segmentarea LAN** în mai multe domenii de coliziune, folosind echipamente de tip switch, bridge și/sau ruter, interconectate prin intermediul unei magistrale de date (*backbone*) la nivelul căreia se definește un alt domeniu de coliziune, distinct de cele asociate segmentelor de rețea formate.

VI.1 PUNȚI DE REȚEA (BRIDGE)

BRIDGE-ul sau **puntea** dintr-o rețea de calculatoare este un dispozitiv care lucrează pe subnivelul MAC al modelului OSI fiind denumit și **releu de nivel 2** (*Layer 2 Relay*). Acesta interconectează mai multe segmente de LAN pentru a realiza o rețea locală extinsă (*Extended LAN*), cu mai multe noduri decât numărul maxim prevăzut de standardele de rețea, respectiv la

distanțe mai mari decât cele impuse prin limitările cauzate de caracteristicile fiecărui mediu fizic de transmisie (lungime maximă a segmentului de cablu; număr maxim de segmente interconectate prin repetoare sau hub-uri conform regulii Ethernet 5-4-3 etc).

Bridge-ul lucrează pe nivelul legăturii de date cu cadre de date (*data frame*), deci în mod transparent față de protocoalele definite pe nivelele OSI superioare și independent de protocoalele de rețea aplicate.

Accesul la mediul fizic de transmisie se realizează în baza standardului de rețea utilizat deci este posibil să apară întârzieri în transferul cadrelor prin punte fiind necesară stocarea lor. Puntea citește câmpurile de adresă MAC ale sursei și destinației și retransmite fiecare cadru către rețeaua în care se găsește destinația (*store-and-forward*). Este posibilă filtrarea inteligentă a cadrelor pe baza adreselor MAC ceea ce permite reducerea încărcării rețelelor, creșterea lățimii de bandă disponibile, controlul accesului și securizarea transmisiei la nivelul punții.

O punte poate interconecta segmente de LAN având medii fizice de transmisie diferite (UTP, cablu coaxial, fibră optică) dar lucrând pe baza aceluiași protocol de nivel 2 (de exemplu Ethernet: 10 BASE T; 10 BASE 2; 10 BASE 5 etc).

O punte este prevăzută cu diferite porturi fizice care pot asigura fiecare accesul multiplu la nivelul lor, dacă se configurează în mod adecvat cu mai multe interfețe logice (*ppp; fr*).

Dacă puntea dispune de un port pentru legătură în WAN, atunci ea poate fi utilizată pentru realizarea unui LAN extins din mai multe rețele locale din WAN, separate geografic, și configurată 'de la distanță' (*remote bridge*).

În figura VI.1 este reprezentată o rețea locală extinsă cu punți. Fiecare punte permite intrarea sau transferul cadrelor din rețeaua centrală în cea locală numai dacă destinația aparține acesteia. În caz contrar cadrul nu este trecut prin bridge. De asemenea, un cadru trimis din LAN-ul propriu este transferat de punte în rețeaua de legătură, pe magistrala de date de mare viteză (*backbone*), numai dacă destinația nu se găsește în același LAN cu sursa.

De exemplu, un mesaj transmis de stația A1 pentru stația C2 va fi transferat prin puntea B1 în rețeaua de legătură, preluat de puntea B2 și retransmis stației C2.

Mesajul nu trece prin puntea B3. Dacă se face o transmisie între două terminale din interiorul aceluiași LAN, atunci cadrul nu este transferat de puntea proprie în rețeaua centrală.

Puntea memorează adresele nodurilor din rețeaua locală proprie într-un tabel de adrese.

Tabelul punții conține numele interfețelor și adresele fizice ale echipamentelor direct conectate la fiecare dintre acestea.

Dacă adresa destinației nu este cunoscută, atunci mesajul respectiv este transmis prin broadcast către toate stațiile.

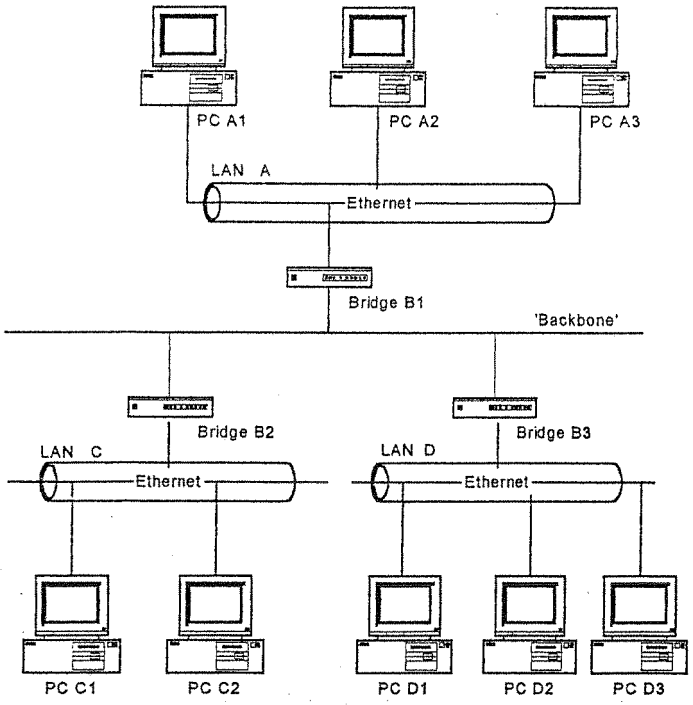


Fig. VI.1 Exemplu de LAN extins cu punți

În situația în care adresa destinației este inexistentă și există bucle în topologia rețelei, mesajul se poate propaga la infinit, producând așa-numitul fenomen de 'furtună de difuzare' (*broadcast storm*). Acest fenomen este mai puternic dacă un mesaj este destinat unui nod care nu aparține rețelei proprii și este trecut prin mai multe punți către așa-zisa destinație. Broadcast-ul se realizează atunci la nivelul fiecărei punți și fenomenul ia amploare. Deducem că punțile sunt ineficiente și chiar neindicate în rețelele cu topologie redundantă.

În rețelele de arie largă cu topologie fizică de tip 'plasă' (*mesh*), unele punți permit utilizarea căilor multiple (redundante) de transmisie și alegerea căii optime dintre sursă și destinație aplicând algoritmul de deducere a drumului minim dintr-un graf (*STA Spanning-Tree Algorithm*). De asemenea, pentru WAN, se pot defini la nivelul punții ierarhii de priorități pentru reducerea întârzierilor de transmisie a anumitor cadre.

Comutarea de pachete prin intermediul punților de transmisie se realizează prin algoritmi software, ceea ce determină apariția unor întârzieri de transmisie cauzate de procesele logice de

decizie. Segmentarea rețelelor locale cu punți determină o creștere a timpului de transmisie de până la 30 %. Avantajoasă este posibilitatea definirii filtrelor de trafic la nivelul punții.

Spre deosebire de punțile de rețea, comutarea de pachete prin switch este un proces relativ rapid care se realizează prin intermediul unei structuri hardware (matricea de comutație) la care calculatoarele sunt direct conectate. Ca dezavantaje ale utilizării switch-urilor se observă formarea mai multor domenii de coliziune dar menținerea unui singur domeniu de braodcast și imposibilitatea limitării vitezei de trafic prin switch. Ca avantaje trebuie remarcate viteza mare de comutare și posibilitatea definirii rețelelor locale virtuale (VLAN - *Virtual LAN*).

Procesul de comunicație prin punte (*bridging process*) este complex și se realizează în două etape:

1. **procesul de învățare** (*learning process*) se realizează în mod adaptiv și constă în 'învățarea' adreselor MAC ale tuturor stațiilor dintr-un LAN extins. La primirea unui cadru, puntea caută adresa MAC a sursei în harta stațiilor (*station map*) și dacă nu o găsește, atunci o include în aceasta. Se inițializează contorul pentru măsurarea duratei intervalului de timp în care puntea cunoaște această adresă (*aging timer*). Contorul este reinițializat de fiecare dată când se recepționează o adresă cunoscută. La expirarea acestui timp, adresa stației respective este ștearsă din harta stațiilor. Orice cadru recepționat care are adresa de destinație cunoscută (inclusă în harta stațiilor) este transmis pe portul corespunzător stației respective.

2. **procesul de transferare** (*forwarding process*). Orice cadru recepționat este preluat de punte cu condiția ca adresa destinației să aparțină LAN-ului respectiv și numai dacă portul pe care a fost primit este în starea activă (*forwarding state*). Dacă adresa destinației apare în harta stațiilor atunci cadrul este transferat pe portul respectiv. În cazul în care adresa destinației nu este inclusă în harta stațiilor, cadrul este retransmis pe toate porturile punții (*flooding*) cu excepția celui de pe care a fost recepționat. Cadrul este transferat de un port numai dacă acesta este activ. În caz contrar, cadrul este descărcat din memoria punții și datele se pierd. Procesul de transfer a cadrelor prin punte poate fi controlat prin filtrare. Rata de transfer a cadrelor la nivelul punții poate avea valori cuprinse între 700 și 30.000 pachete pe secundă.

Porturile unei punți, definite ca tip și număr, pot să se găsească în una din următoarele cinci stări:

1. **starea inactivă** (*disabled*) - nu se face nici o operație la nivelul portului;
2. **starea de 'ascultare'** (*listening*) - se pot recepționa cadre;
3. **starea de 'învățare'** (*learning*) - se recepționează cadrele și se realizează harta stațiilor;
4. **starea activă** (*forwarding*) - se recepționează și se transferă cadre prin portul respectiv iar algoritmul *'spanning tree'* este activat;

5. **starea de blocare** (*blocking*) - transferul de cadre prin port este inactiv dar algoritmul '*spanning tree*' este activ pentru operare la nivelul portului.

Există punți care permit 'la cerere' (*on-demand bridge*) realizarea transmisiilor de tip '*broadcast*' sau '*multicast*'. Acest fapt poate conduce la încărcarea excesivă a rețelelor ceea ce impune configurarea adecvată a echipamentelor pentru filtrarea severă a traficului. În acest caz nu se aplică algoritmul '*spanning tree*'.

Urmărirea funcționării unei punți se face cu protocoale de management de rețea (SNMP) folosind baze de date separate (MIB).

Clasificarea punților se poate face pe mai multe criterii.

În funcție de arhitectura LAN utilizată, punțile se împart în:

1. **punți transparente** (*transparent bridges*) care interconectează segmente de LAN cu același protocol la nivelul legăturii de date;

2. **punți de translare** (*translating bridge* sau *multiprotocol bridge*) care realizează conversia formatului cadrului de date dintr-un standard în altul (de exemplu, Ethernet și Token-Ring) și sunt prevăzute cu mai multe plăci de rețea.

3. **punți de încapsulare** (*encapsulating bridge*) pentru interconectarea unui LAN Ethernet cu unul FDDI.

În funcție de localizarea lor, punțile pot fi:

1. **punți locale** (*local bridge*) care interconectează două LAN-uri direct printr-un anumit mediu de transmisie. Acestea conțin mai multe plăci de rețea și pot face conversia de la un mediu la altul.

2. **punți 'la distanță'** (*remote bridge*) conțin plăci de rețea pentru conectarea la diverse LAN-uri precum și porturi de acces 'la distanță' în WAN prin modemuri și un port serial (RS-232). Ele realizează compresia datelor pentru reducerea lățimii de bandă ocupate, sunt monitorizate prin SNMP și suportă Telnet pentru configurarea lor 'de la distanță'.

În rețelele WAN 'fără fir' (*wireless*) se utilizează perechi de **punți de transmisie 'fără fir'** (*wireless bridge*) pentru legături la distanțe mari (de peste 5 km), care suportă STA, filtrare bazată pe adrese MAC, SNMP, criptare de date și protecție contra fenomenului '*broadcast storm*' .

Performanțele unei punți se apreciază prin următorii parametri:

1. **rata de transfer fără erori;**

2. **rata de pierdere a pachetelor;**

3. **întârzierea de transmisie** (se minimizează prin folosirea unui procesor rapid de comunicație în punte).

Configurarea prin soft a unei punți include:

1. definirea porturilor, fizice, respectiv logice (de exemplu: *eth0; eth1; ppp0; ppp1; ppp2*) ;

2. definirea protocoalelor pentru care se aplică procesul de '*bridging*' (*ARP; Novell; AppleTalk* ș.a.), eventual activarea algoritmului '*spanning tree*';

3. definirea grupurilor de utilizatori;

4. definirea filtrelor de includere a utilizatorilor autorizați sau de excludere a anumitor cadre (de exemplu, încapsulate conform anumitor standarde sau de dimensiuni prea mari). Rata de filtrare a unei punți variază de la 7000 la 60.000 de cadre pe secundă.

Se utilizează diverse comenzi de configurare a punților, cu sintaxa definită de firma producătoare a echipamentelor:

- de activare a punții (enable bridge);
- de activare a algoritmului de deducere a drumului minim prin graf (enable bridge spanning);
- de definire a interfețelor logice și fizice (create; add);
- de definire a protocoalelor recunoscute de punte (add bridge protocol), tipul protocolului fiind specificat printr-un număr de patru cifre din sistemul hexazecimal.
- de introducere a unot filtre de transmisie (add bridge filter);
- de vizualizare a modului de configurare (show).

Observație

Fișierele de configurare pot fi încărcate în memoria echipamentelor folosind TFTP ca protocol de transfer.

VI.2 ECHIPAMENTE DE DIRIJARE (ROUTER)

Echipamentul de dirijare (*router*) este un echipament de comunicație de nivel rețea (*layer 3 device*) care utilizează algoritmi specifici de deducere a căii optime de transfer a datelor într-o rețea de arie largă având căi redundante, pe baza informațiilor pe care le deține referitor la topologia rețelei.

Rutarea este operația de dirijare a datelor între două noduri prin stabilirea 'drumului minim' din graful asociat topologiei fizice sau celei logice a unei rețele. Astfel routerul maximizează ratele de transfer și de filtrare a pachetelor.

Orice LAN poate comunica într-un WAN dacă este conectat la aceasta printr-un router.

Baza de date în care sunt incluse informațiile despre topologia rețelei poate fi configurată **static**, de către administratorul de rețea, sau **dinamic**, prin intermediul protocoalelor de rutare.

Rutarea statică nu permite reactualizarea la timp a tabelelor de rutare și este practic ineficientă în cazul utilizării protocoalelor de adresare dinamică.

Un router poate transfera date între LAN-uri diferite ca standard de transmisie (Ethernet, FDDI, ATM) fiind prevăzut cu diverse interfețe având adrese individuale. Routerele pot face conversiile necesare ale formatului pachetelor în cazul interconectării unor segmente de rețea cu standarde și protocoale diferite.

Observație

Routerele sunt prevăzute atât cu interfețe fizice, cât și cu interfețe logice, de exemplu, interfețe *ppp* definite prin protocolul PPP *(Point-to-Point Protocol)* în cazul transmisiilor TDM, având alocate adrese de nivel rețea proprii (de exemplu, adrese IP) pe baza cărora se realizează rutarea pachetelor. PPP, ca protocol de nivel OSI 2, încapsulează în mod transparent datagramele transmise pe legături seriale lucrând ca multiplexor/demultiplexor pe aceste linii. PPP (RFC 1717) este responsabil de aplicarea protocoalelor de autentificare PAP (*Password Authentication Protocol*) și CHAP (*Challenge Handshake Authentication Protocol*). PPP negociază cu utilizatorii numele și parolele dar există riscul interceptării lor întrucât nu sunt transmise criptat. Între routerele aflate la 'distanță' se pot aplica procedee de criptografiere a acestor informații. Este indicată schimbarea periodică a parolelor.

Rutarea pachetelor, mai precis transferul pachetelor în interiorul ruterului către un anumit port de ieșire din router se face pe baza **tabelului de rutare,** care asociază adresele de rețea ale rețelelor de destinație posibile cu interfețele de ieșire din router. Routerul realizează deci operația de comutare a pachetelor (*switching*) pe interfața corespunzătoare. Pentru adrese de destinație neincluse explicit în tabelul de rutare, se definește o rută implicită (*default route*).

Exemplu:

În figura VI.2, LAN A transmite date către LAN B.

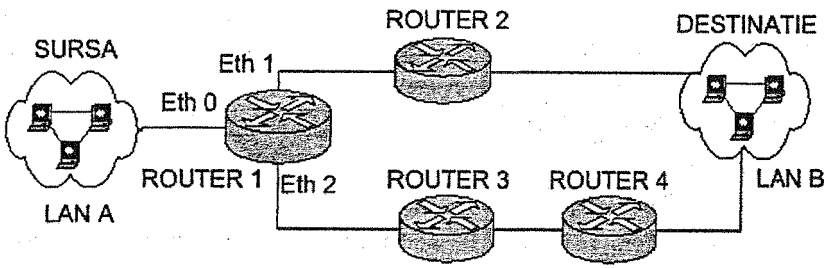


Fig.VI.2 Exemplu de LAN-uri interconectate cu routere în WAN

LAN A este conectat la interfața *Eth 0* a ruterului 1.

Pentru LAN B ca destinație, în tabelul de rutare al ruterului 1, se includ două căi, prin interfața *Eth1*, respectiv prin *Eth2*, cu precizarea căii optime (Tabel VI.1).

Tabel VI.1

Intrări în tabelul de rutare definit pentru routerul 1

LAN destinație	Interfață de ieșire	Optim
LAN B	*Eth1*	+
LAN B	*Eth2*	-

Se observă că în graful rețelei de comunicații (cu routere) nu apar bucle. Routerul transmite pachetul pe ruta optimă, cea de rezervă urmând a fi utilizată în cazul întreruperii traficului pe prima rută.

Din cadrul recepționat se extrage pachetul și se citește adresa de nivel OSI 3 a stației de destinație. Aplicându-se acesteia masca de rețea se deduce adresa rețelei de destinație, urmând să se ia decizia de comutare pe o anumită interfață a ruterului prin deducerea rutei optime.

Se folosește o anumită metrică pentru stabilirea 'drumului minim' dintre două noduri din graful rețelei (număr de routere sau 'hopuri' prin care se face transferul, întârziere de transmisie, risc minim de coliziune etc). La nivelul interfeței de ieșire, pachetul este reîncapsulat într-un cadru, conform standardului de nivel OSI 2 aplicat pe acea interfață. În rețelele WAN mixte (de exemplu, Ethernet și Token-Ring) se poate folosi același protocol de nivel-rețea (de exemplu, IP) și același mod de adresare de nivel OSI 3, dar formate diferite pentru cadrele definite pe nivelul OSI 2.

De fiecare dată când topologia rețelei se modifică (prin dezvoltarea sau reconfigurarea rețelei ori cauzat de coliziunile din trafic), este necesară reactualizarea tabelelor de rutare (*reconvergence*). Timpul de reconversie a tabelelor depinde de protocolul de rutare aplicat. Dacă routerele din WAN nu dispun toate de aceleași informații topologice, atunci este posibil să se ia decizii de rutare incorecte sau inaplicabile. Dacă un router nu poate expedia un pachet (*destination unreachable*), atunci se transmite către sursă un mesaj de eroare (de exemplu, prin intermediul ICMP).

Protocoalele care utilizează modul de adresare ierarhizat definit pe nivelul OSI 3 se numesc **protocoale rutabile.**

De exemplu, IP, FTP, IPX, AFP (AppleTalk) sunt protocoale rutabile.

Orice protocol care nu utilizează adrese definite pe nivelul de rețea este considerat **protocol nerutabil.** De exemplu, protocolul NetBeui utilizat pentru managementul unui LAN este nerutabil și pachetele transmise de acesta vor fi transferate de router prin procedeul de bridging.

Dacă într-o rețea un anumit protocol (de exemplu, IP) este definit ca protocol rutabil, atunci cadrele transmise de un router IP definite cu un protocol nerutabil (cadrele non-IP) vor fi retransmise de acesta prin procesul de '*bridging*'.

Un router definit pe un singur protocol de rețea are avantajul că știe exact unde se găsește în pachet adresa destinației și procesează rapid datele. În plus, prin citirea tipului protocolului de rețea în cadrul de date (de exemplu, în cadrul Ethernet), routerul poate transfera datele numai în rețeaua care lucrează cu acel protocol. Astfel se reduce încărcarea rețelei și se pot defini priorități de transmisie.

Routerele multiprotocol lucrează cu structuri diferite de pachete, cu diverse formate ale adresei de destinație, ceea ce îngreuiază procesul de rutare și determină întârzieri de transmisie mai mari (30% - 40%). De aceea, în multe cazuri, se preferă interconectarea LAN-urilor cu switch-uri de nivel 3 sau 4.

Observații:

1. Un router, deși este un echipament de comunicație de nivel 3, poate fi configurat să lucreze și ca bridge (*BR - BRouter*).

2. Un router poate lucra ca 'zid de protecție' (*firewall*) între două LAN-uri interconectate pentru eliminarea transmisiilor broadcast nedorite și a fenomenului de saturare a rețelelor (*flooding*), pentru securizarea traficului de pachete și asigurarea transparenței legăturii.

3. Segmentarea rețelelor cu routere este mai avantajoasă decât cea realizată cu bridge-uri sau switch-uri, deoarece se lucrează cu adrese de rețea, respectiv cu o schemă de adresare ierarhizată, pe domenii de coliziune mai mici, aplicând un algoritm de deducere a rutei optime ceea ce asigură fluența traficului și minimizează riscul de coliziune, dar determină unele întârzieri de transmisie.

4. Routerele nu transmit cadre prin broadcast pe baza adreselor fizice (de exemplu, ARP), ceea ce reduce încărcarea rețelelor. Astfel routerele delimitează domeniile de broadcast.

5. Routerele pot fi configurate software, prin comenzi specifice, definite de firma producătoare.

VI.3 PROTOCOALE DE RUTARE

Protocoalele de rutare stabilesc mecanismul prin care routerele obțin informațiile referitoare la topologia rețelei (de exemplu, RIP - *Routing Information Protocol;* IGRP - *Internal Gateway Routing Protocol;* EGRP - *Enhanced IGRP*; OSPF - *Open Shortest Path First* etc).

Aceste protocoale permit actualizarea tabelului de rutare al fiecărui router și transmisia informațiilor referitoare la modificările survenite în acesta către routerele învecinate.

Clasificarea protocoalelor de rutare se poate face pe baza criteriului de deducere a rutei optime:

1. **vectori de distanță** (ex. RIP; IGRP);

2. **starea legăturii** (OSPF);

3. **combinații între vectorii de distanță și starea legăturii** (protocoale hibride, de exemplu EGRP).

O altă clasificare a protocoalelor de rutare se face în funcție de aria de acoperire a acestora.

Dacă rețeaua WAN este divizată în mai multe sisteme autonome (AS - *Autonomous System*), atunci comunicația dintre routerele din interiorul acestora se face cu **protocoale de rutare interne** (de exemplu, RIP, IGRP) iar între routerele care asigură comunicația dintre sistemele autonome se utiizează **protocoale de rutare externe** (ex: EGP - *External Gateway Protocol*; BGP - *Border Gateway Protocol*) (Fig.VI.3).

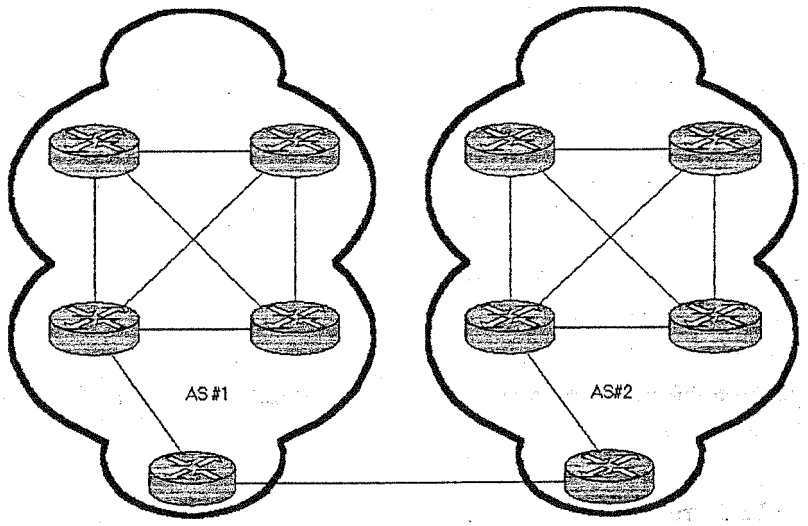


Fig.VI.3 Interconectarea unor sisteme autonome

VI.3.1 Protocoale de rutare cu vectori de distanță

Protocoalele de rutare cu vectori de distanță impun transmisia periodică către toate routerele învecinate a informațiilor de rutare utilizate de un router. Astfel se reactualizează bazele de date care conțin informațiile referitoare la topologia rețelei.

Fiind un proces de tip "pas-cu-pas", rutarea cu vectori de distanță nu asigură o cunoaștere exactă a topologiei rețelei iar reactualizarea tabelelor de rutare se face relativ lent.

Un router **RIPv1** (*Routing Information Protocol version 1*) transmite prin broadcast, la fiecare 30 secunde, un mesaj de înștiințare (*hello*) către toate routerele adiacente din WAN, specificând pentru fiecare rețea de destinație, distanța până la aceasta ca număr de hopuri (de exemplu, maxim 15). Astfel tabelele de rutare sunt reactualizate. Protocolul nu lucrează la nivel de subrețele. Pachetele IP transmise își decrementează timpul de viață la trecerea printr-un router urmând să fie distruse atunci când timpul pentru transfer expiră. RIPv1 este considerat protocol de rutare statică.

Protocolul **RIPv2** (RFC 1723), permite aplicarea măștilor de subrețea și includerea subrețelelor în tabelul de rutare. Acest protocol dinamic poate fi utilizat și în interiorul LAN-ului pentru interconectarea subrețelelor folosind un router intern deci este de tip IGRP (*Internal Gateway Routing Protocol*).

Protocolul **DVMRP** (*Distance Vector Multicast Routing Protocol*) este orientat pe ariile de acoperire ale ruterelor ceea ce presupune că modificările intervenite în tabelele de rutare sunt comunicate prin multicast numai ruterelor din aria respectivă. După expirarea timpului de viață, anumite linii din tabelul de rutare sunt eliminate. Protocolul poate fi aplicat pe subrețele. Fiind un protocol bazat pe vectori de distanțe, nu evită blocajele de trafic. Vectorii de distanță sunt calculați pe diferite grafuri de rețea, cu metrici diverse (întârziere de transmisie, siguranță, costuri etc) ceea ce permite deducerea rutei optime în funcție de opțiunile exprimate în pachetele de date.

Uneori volumul informațiilor de rutare poate fi relativ mare și este eficientă gruparea rutelor corespunzătoare diferitelor adrese de destinație în entități mai mari, prin procedeul CIDR (*Classless Interdomain Routing*).

VI.3.2 Protocoale de rutare bazate pe starea legăturii

Protocoalele de rutare care utilizează starea legăturii mențin la nivelul fiecărui router o bază de date complexă, cu informații despre toate routerele din rețea, nu numai despre cele învecinate. Pe baza grafului rețelei, se aplică algoritmul de deducere a căii minime și se stabilește ruta optimă

pentru fiecare rețea de destinație. În cazul schimbării topologiei rețelei, actualizarea tabelelor de rutare se face relativ rapid.

Protocolul de rutare dinamică **OSPF** (*Open Shortest Path First*) se aplică în rețelele mari ca număr de noduri, inclusiv pe subrețele, cu autentificarea datelor, iar rutarea și rerutarea pachetelor se face mai rapid decât prin RIP, definindu-se arii de acoperire pentru fiecare router. Acest protocol este de tip IGRP și a fost special proiectat pentru rutare în rețelele care utilizează TCP/IP. Fiecare router intern din sistemul autonom (AS - *Autonomous System*) deține o bază de date proprie în care sunt incluse informații privind starea interfețelor ruterului, routerele vecine și altele. Routerele vecine se informează reciproc prin *flooding* numai dacă apar modificări în tabelele proprii de rutare, în care se precizează pentru fiecare rută, suplimentar față de RIP, costul și lățimea de bandă disponibilă. Interconectarea ariilor de acoperire din sistemele autonome, se face prin intermediul unor routere AS desemnate (*boundary router*) iar între AS-uri se utilizează **routere externe** (*external router*) care permit transferul unor pachete la distanțe mari în WAN. Deducerea rutei optime se face pe baza unor arbori de acoperire a AS, în care nu apar bucle iar routerele externe sunt noduri terminale în 'arbore'.

Calea spre destinație poate fi de tip:

1. INTRA - în interiorul unei singure arii din AS;

2. INTER - traversează mai multe arii din același AS fără a traversa un router de la granița AS;

3. EXT1 - calea trece printr-un router din AS și rămâne în interiorul AS. Se utilizează două metrici, metrica OSPF internă și cea a routerului AS, pentru a deduce ruta optimă.

4. EXT2 - calea trece dintr-un AS în altul printr-un router extern, deci se combină metrica OSPF internă cu cea a routerului EGP (*External Gateway Protocol*) pentru găsirea rutei optime.

Protocoalele RIP sunt orientate pe vectori de distanță și utilizează numai informațiile furnizate de routerele adiacente, în timp ce OSPF este orientat pe starea legăturii dintre noduri (LST - *Link State Technology*) și permite optimizarea transferului pe baza informațiilor deținute de toate routerele din WAN. Routerele OSPF admit importul și exportul de informații din și spre un router RIP.

VI.3.3 Rutarea IP

Un router definit pentru IP este numit **router IP** sau **gateway** (' poartă' de transmisie). În prezent, un gateway poate lucra și la nivelele superioare celui de rețea din modelul OSI, termenul fiind utilizat într-un sens mult mai larg decât cel de router IP.

Rutarea IP se poate face în două moduri:

1. **static**, caz în care administratorul de rețea introduce manual rutele în tabelul de rutare, specificând pentru fiecare adresă a rețelei de destinație:

- adresa interfeței de ieșire din router;
- adresa următorului router (*next Hop*);
- eventual metrica de cale.

Rutarea se face simplu, pe baza tabelului de rutare. Din adresa destinației, prin aplicarea măștii de rețea, se deduce adresa rețelei de destinație și pachetul este transferat pe portul de ieșire corespunzător. Metoda nu asigură deducerea căii optime și nu elimină riscul congestiilor de trafic.

2. **dinamic**, prin reactualizarea tabelelor de rutare atunci când apar modificări ale adreselor rețelelor sau subrețelelor, ale metricii utilizate sau coliziuni în WAN. Acest mod de rutare permite deducerea căii optime dintre rețeaua-sursă și cea destinație pentru reducerea timpului, a costurilor de transmisie sau a riscului de coliziune.

Rutarea IP dinamică presupune alegerea protocolului de rutare (de exemplu, RIP, OSPF), stabilirea adreselor și a măștilor de rețea pentru toate rețelele direct conectate la acel router.

Întrucât spațiul de adrese IP este limitat, în numeroase rețele se alocă utilizatorilor adrese IP private care nu trebuie confundate cu adresele IP reale (*public*) alocate de InterNIC. Rutarea pachetelor se face pe baza adreselor IP reale alocate interfețelor ruterelor de ieșire în WAN, folosind procedeul NAT de translare a adreselor.

Pentru rutarea cu adrese private, se încapsulează pachetele IP transmise în Internet cu antete suplimentare prin așa-numitul **mecanism GRE** (*Generic Routing Encapsulation*), descris în RFC 1701. Pachetului inițial (*payload packet /original packet*) i se adaugă un antet GRE (*GRE Header*) și un antet privind modul de transfer specificat conform protocolului de rețea (*delivery header*) (Fig.VI.4).

Antet de transmisie	Antet GRE	Pachet original

Fig. VI.4 Încapsularea GRE

Prin GRE se asigură transparența adreselor intermediare și securitatea transmisiei, prin realizarea unui așa-numit "tunel de transmisie" (*tunnelling*) .

Uzual este cazul încapsulării pachetelor IP pentru transmisii cu IP (*IP over IP*) conform RFC 1702, standard definit pentru GRE.

Conform RFC 1597, anumite spații de adrese IP din clasele A, B și C sunt rezervate pentru procedeul GRE și sunt numite **adrese private** (*private*):

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255.

Aceste adrese IP pot fi utilizate în încapsularea GRE astfel încât cadrul să fie interpretat ca fiind încapsulat GRE și routerele 'de la distanță' să extragă adresa de destinație privată din pachetul original.

Exemplu

Să presupunem existența a două rețele locale de calculatoare A și B având alocate adresele IP private 192.168.3.0 și 192.168.4.0.

Aceste rețele sunt conectate în WAN prin intermediul a două routere cu adresele IP publice alocate interfețelor: 193.162.35.110 și 195.16.23.12.

Cele două routere comunică prin intermediul unui al treilea router cu adresa 194.225.140.1.

Un pachet trimis de la adresa 192.168.3.2 către 192.168.4.5 va fi încapsulat prin procedeul GRE specificându-se în antetul de transmisie numai adresele IP private ale routerului-sursă și respectiv routerului-destinație fără a se menționa adresa routerului intermediar. Adresa acestuia este inclusă doar în tabelele de rutare nefiind vizibilă din exterior. Urmează ca în LAN-ul B să se extragă datele și să se citească adresa IP alocată local destinației .

Observații:

1. Există protocoale similare celor de rutare IP pentru rețelele care folosesc IPX/SPX, DECnet sau AppleTalk, eventual cu alte valori ale intervalelor de timp privind reactualizarea informațiilor (de exemplu, routerele IPX RIP transmit prin broadcast informațiile lor de stare la fiecare 60 de secunde). Fenomenul de broadcast este dificil de administrat în rețelele comutate (ISDN).

2. SAP (*Server Advertising Protocol*) este utilizat în rețele Novell, pentru transmisia periodică prin broadcast a informațiilor privind rutarea către serverele din rețea, la fiecare 60 de secunde. Routerele construiesc tabelele SAP pe care le transmit celorlalte routere din WAN, urmând ca fiecare să transmită aceste informații prin broadcast în LAN-uri, la servere.

3. Routerele IP admit definirea rețelelor locale virtuale (VLAN - *Virtual LAN*), constând în gruparea logică a nodurilor rețelei, fără a ține cont de segmentul fizic de care aparțin. În rețelele Ethernet și Fast Ethernet bazate pe VLAN-uri, se utilizează protocolul STP (*Spanning-Tree Protocol*), pentru a elimina buclele din graf și a evita apariția fenomenului "*broadcast storm*", care determină creșterea la infinit a numărului pachetelor transmise prin broadcast într-o rețea redundantă. STP configurează porturile pentru a realiza transferul sau blocarea pachetelor pe anumite căi.

VI.4 REȚELE LOCALE VIRTUALE (VLAN)

O rețea locală virtuală (VLAN - *Virtual Local Area Network*) reprezintă gruparea logică a componentelor unei rețele locale, fără a ține cont de gruparea lor fizică.

Segmentarea fizică a unui LAN cu echipamente de comunicație de tip hub, switch, sau bridge face posibilă segmentarea domeniului de coliziune inițial în mai multe domenii de coliziune, dar păstrează un singur domeniu de broadcast, ceea ce permite un control mai eficient al congestiilor din rețea dar nu reduce încărcarea rețelei prin transmisia mesajelor de broadcast.

Routerul este singurul echipament care delimitează un domeniu de broadcast, îndeplinind funcția de așa-numit "zid-de-foc" (*firewall*) (Fig. VI.5).

În multe cazuri este utilă gruparea calculatoarelor-gazdă în domenii de broadcast separate, pe diferite criterii independent de conexiunile fizice existente în rețea și de amplasarea lor în spațiul unei clădiri sau a unui campus.

Într-o clădire sau într-un grup de clădiri, se pot defini grupuri de utilizatori cu preocupări similare. De exemplu, departamentul comercial al unei societăți poate să includă calculatoare situate pe diferite nivele ale aceleiași clădiri sau în mai multe corpuri de clădire.

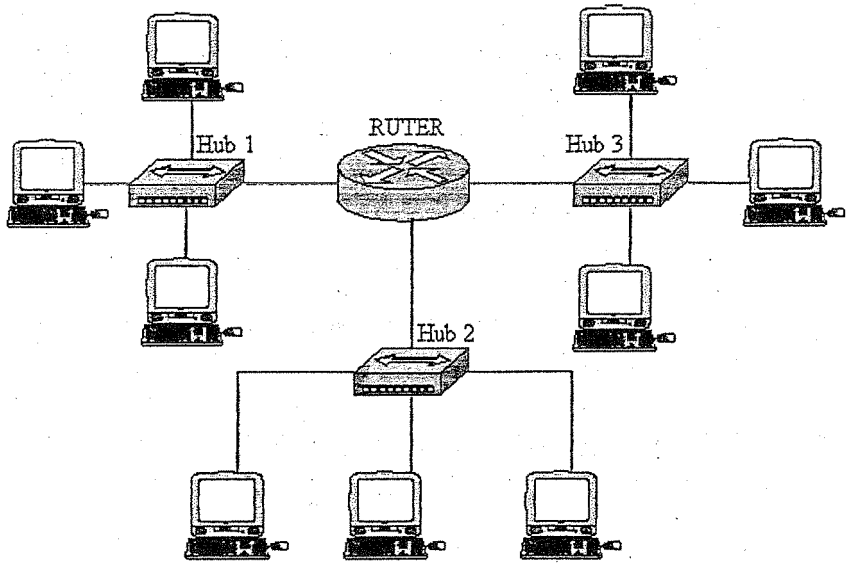


Fig. VI.5 Rețea locală segmentată cu un router

Acestea trebuie să acceseze o bază de date unică, cu informații specifice și în același timp trebuie creată posibilitatea difuzării unor mesaje prin broadcast, către toți utilizatorii din acel departament. Accesul din afara grupului respectiv trebuie restricționat. Similar se pot defini grupuri de utilizatori care lucrează în departamentul tehnic, în cel administrativ sau în cel financiar. Se obțin astfel mai multe grupuri de utilizatori și mai multe rețele locale virtuale, cu domenii de coliziune și de broadcast independente: VLAN 1, VLAN 2, VLAN 3 și VLAN 4 (Fig. VI.6).

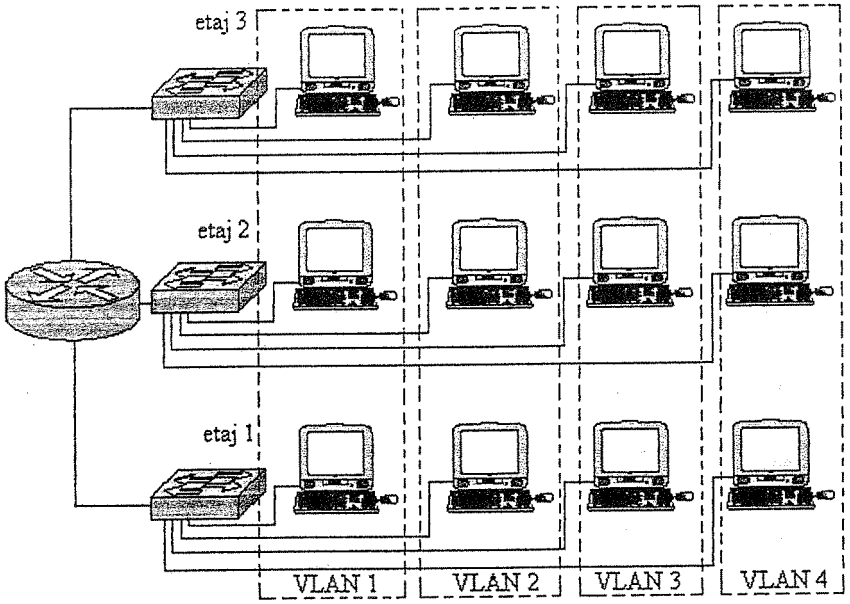


Fig. VI.6 LAN cu patru rețele locale virtuale

Definirea VLAN-urilor se poate face în funcție de diverși factori:

- numere de identificare (ID - *identifier*) a porturilor;
- adrese MAC;
- protocoale de rețea;
- porturi de aplicație.

Fiecare VLAN reprezintă un domeniu de broadcast independent, ceea ce permite reducerea încărcării rețelei prin difuzarea mesajelor către toți utilizatorii.

Se poate defini câte un VLAN pe fiecare port al switch-ului. Mai multe porturi din switch pot să aparțină aceluiași VLAN. La nivelul switch-ului, transmisiile prin broadcast se fac numai pe porturile asociate aceluiași VLAN.

VLAN-urile lucrează pe nivelele OSI 2 și 3. Comunicația între VLAN-uri se face prin rutare, deci pe nivelul de rețea, prin intermediul unui router sau al unui switch de nivel 3.

Includerea utilizatorilor în VLAN-uri se realizează prin soft, cu comenzi specifice incluse în fișierele de configurare a echipamentelor de comunicații din rețea.

Implementarea VLAN-urilor este avantajoasă întrucât schimbarea locației fizice a unui calculator care rămâne în același VLAN nu impune reconfigurarea routerelor și nici modificarea structurii cablate a rețelei. În plus, definirea rețelelor virtuale oferă o securitate mai mare a comunicațiilor din rețea, prin restricționarea accesului între VLAN-uri.

Principiile VLAN pot fi aplicate și în rețelele de arie largă (WAN), prin utilizarea unor magistrale de date de mare viteză (*backbone*) de exemplu, Fast Ethernet, FDDI, ATM.

Există două principii de definire a VLAN-urilor:

1. **Identificarea cadrelor** (*frame tagging*), conform standardului IEEE 802.1q.

La fiecare cadru de date care circulă pe această magistrală între diferite VLAN-uri, se poate atașa un identificator de VLAN pentru dirijarea traficului.

2. **Filtrarea cadrelor** între VLAN-uri (*frame filtering*), pe baza unui tabel de adrese.

În rețeaua prezentată pentru exemplificare în figura VI.7, switch-urile pot filtra cadrele între VLAN-uri pe baza unui tabel de adrese, permanent actualizat folosind informațiile furnizate de sistemul de management al rețelei. Cadrele sunt transferate în VLAN-ul corespunzător, în funcție de adresa MAC de destinație.

Tabel de adrese

Adrese MAC	VLAN
12-aa-54-9f-ee-d5	1
30-46-93-b3-f1-0c	1
25-5b-d3-2e-40-a3	2
d6-55-07-91-42-32	2
52-11-6a-de-2f-50	3
a2-14-fd-d8-10-72	3

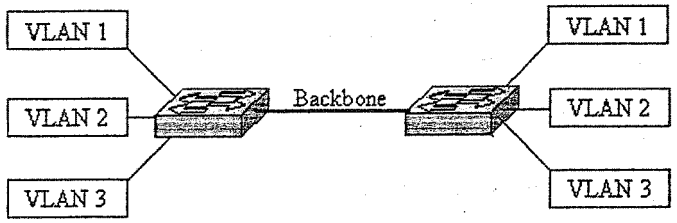


Fig. VI.7 VLAN-uri interconectate de o magistrală de date

Filtrarea cadrelor este o operație complexă și de durată relativ mare. Metoda de proiectare a VLAN-urilor prin identificarea cadrelor se realizează pe nivelul OSI 2 și este mai flexibilă decât cea prin filtrare. Identificatorul de VLAN se atașează în antetul cadrului la intrarea pe magistrala de date și este eliminat la ieșirea din aceasta. Acest identificator se folosește numai între switch-uri sau routere, în backbone, adică în zona de **cablare verticală**, în care se lucrează pe mai multe nivele OSI. Identificatorii de VLAN nu apar în zona de **cablare orizontală**, de comunicație la nivel fizic, între hub-uri și echipamentele terminale (Fig. VI.8).

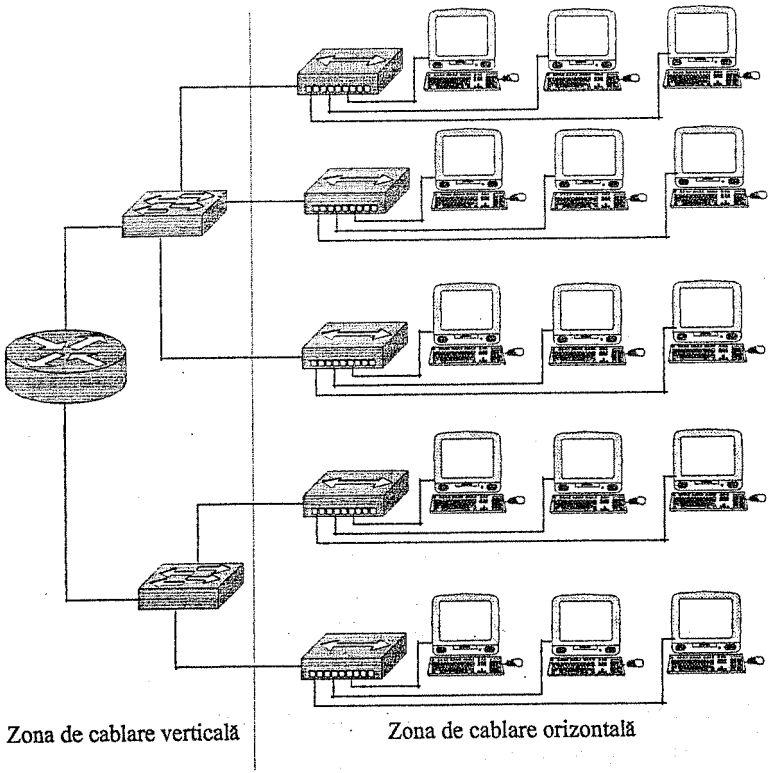


Fig. VI.8 Schemă de conexiuni fizice

Mecanismul de control implementat de switch analizează fiecare cadru și decide operația care trebuie efectuată:

- transfer spre o destinație unică (*forwarding*);
- filtrare (*filtering*);
- difuzare în VLAN-ul corespunzător (*broadcast*).

Analiza cadrului poate include:

- adresa MAC a sursei;
- adresa MAC de destinație;
- tipul protocolului de rețea.

Există trei **metode de implementare a VLAN-urilor**:

I. **Metoda de implementare a VLAN-urilor pe baza porturilor fizice** (*port-centric*) definește VLAN-urile direct, prin asociere cu anumite porturi din switch/router (vezi schema de conexiuni logice din figura VI.9, asociată schemei de conexiuni fizice din figura VI.8).

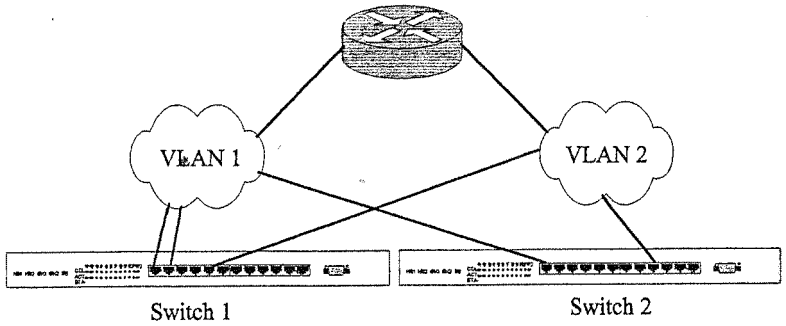


Fig. VI.9 Schema de conexiuni logice de definire a VLAN-urilor

Fiecărei rețele virtuale i se alocă o **adresă de rețea** (de exemplu, într-o rețea bazată pe suita TCP/IP se pot aloca adrese IP de clasă C: 194.125.48.0, 194.125.49.0). Aceste adrese sunt incluse în tabelul de rutare. Routerul interconectează VLAN-urile și dirijează pachetele spre VLAN-ul corespunzător, în interiorul aceluiași VLAN sau între VLAN-uri distincte.

Utilizatorii unui VLAN sunt conectați la porturile fizice din fiecare switch, asociate acelui VLAN.

Metoda este avantajoasă. Administrarea VLAN în acest caz, se face relativ simplu. Securitatea comunicației este crescută. Transmisiile prin broadcast dintr-un VLAN nu afectează celălalt VLAN și în general, pachetele destinate unui VLAN nu sunt transmise și în alte VLAN-uri.

Ca dezavantaj, se observă faptul că un nou utilizator al unui VLAN trebuie conectat fizic în mod obligatoriu la unul din porturile asociate acelui VLAN. Pot să apară deci unele limitări ale capacității rețelei virtuale, ceea ce ar impune modificarea topologiei fizice a rețelei și eventual achiziționarea unor noi echipamente (switch-uri sau huburi de partajare cu număr mai mare de porturi).

II. **Metoda statică** definește VLAN-urile prin asociere cu porturile din switch, gestionarea VLAN realizându-se la nivelul unei **stații de management** și nu la nivelul unui router (Fig. VI.10). Baza de date de management (MIB) a VLAN conține informațiile referitoare la modul de alocare a porturilor din switch-uri rețelelor virtuale.

Asocierea dintre porturi și VLAN-uri se face în mod static, pe baza tabelelor de adrese MAC utilizate de switch-uri. Orice schimbare în topologia rețelei impune intervenția administratorului de rețea pentru actualizarea MIB-ului. Configurarea VLAN-urilor statice este relativ simplă. Comunicația în aceste rețele are un grad mare de securitate.

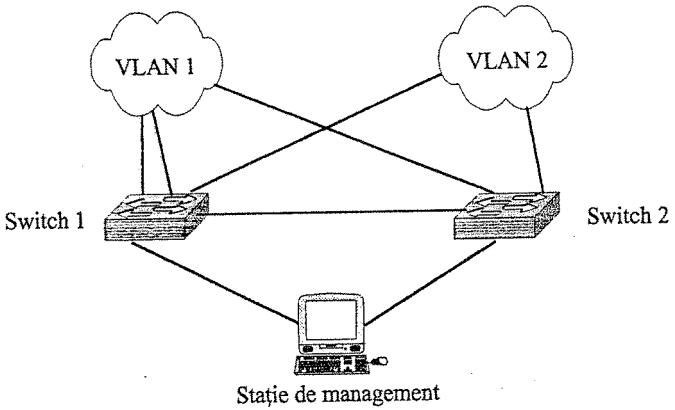


Fig. VI.10 Definirea rețelelor virtuale statice

III. **Metoda dinamică** descrie modul de implementare a VLAN-urilor dinamice, folosind baze de date, memorate și actualizate automat într-un **server de configurare a VLAN-urilor**, fără intervenția administratorului de rețea. Acesta răspunde doar de faza inițială de creare a structurii bazei de date.

Fiecare utilizator, identificat prin adresa sa MAC, poate fi inclus într-un anumit VLAN prin conectare fie la un port deja configurat ca fiind asociat unei rețele virtuale, fie la un port neconfigurat anterior.

Metoda dinamică de definire a VLAN-urilor admite asocierea aceluiași port fizic succesiv cu diferite VLAN-uri. Se păstrează însă restricția că portul nu poate fi asociat cu mai multe VLAN-uri simultan.

Informația de configurare a VLAN-urilor este stocată în baza de date a serverului pentru VLAN care comunică cu toate routerele din rețea pentru actualizarea informațiilor de rutare.

VLAN-urile dinamice se pot defini nu numai pe baza adreselor fizice, dar și a celor de rețea sau a protocoalelor de rețea utilizate.

În cazul conectării unui nou utilizator la un port neconfigurat anterior, se verifică adresa utilizatorului și se configurează dinamic portul respectiv folosind informațiile din baza de date pentru VLAN-uri.

Observații:

1. Un port utilizat inițial pentru un VLAN poate fi reconfigurat ulterior pentru alt VLAN, fără a fi necesară intervenția administratorului de rețea pentru reconfigurarea ruterelor.
2. VLAN-urile pot împărți același spațiu de adrese, de exemplu adrese IP de rețea sau de subrețea.

Definirea rețelelor locale virtuale are o serie de avantaje:

- În aplicațiile curente, topologiile fizice și/sau logice ale rețelelor sunt deseori modificate, ceea ce impune în multe cazuri schimbarea structurii cablate, achiziția de noi echipamente de comunicații (hub, switch etc), reconfigurarea echipamentelor de tip bridge sau router, modificarea bazelor de date de management. Definirea VLAN-urilor determină **reducerea costurilor și eforturilor dedicate schimbărilor din topologia rețelelor.**
- Transmisiile broadcast apar nu numai ca utilitate (de exemplu în aplicațiile de tip multimedia), dar și prin funcționarea defectuoasă a unor componente din rețea (viruși de rețea, furtuni de difuzare etc). Prin divizarea domeniului de broadcast fie la nivelul ruterelor (*firewall*), fie prin definirea VLAN-urilor, **se reduce substanțial încărcarea rețelei.**
- Rețelele locale de calculatoare nu sunt suficient securizate pentru accesul din interior al unui intrus și sunt relativ ușor de penetrat din exterior. Implementarea VLAN-urilor permite **creșterea gradului de securitate a rețelei.** Securizarea VLAN-urilor dedicate anumitor aplicații sau resurse se face prin prin restricționarea numărului de utilizatori din fiecare rețea, separarea domeniilor de broadcast, verificarea oricărui nou utilizator al rețelei. Este absolut necesar să se includă toate porturile switch-urilor neincluse în alte VLAN-uri într-un VLAN simbolic, nedecicat.

Suplimentar, la nivelul ruterelor se pot defini **liste de control a accesului** (ACL - *Access Control List*) pe diferite criterii:

- adrese fizice;
- adrese de rețea;
- protocoale;
- tipul aplicației.

Din motive de securitate se poate recurge la restricționarea accesului în VLAN pe baza listelor de acces, eventual și în funcție de anumite intervale orare.

Observație:

Se pot implementa și rețele virtuale private (VPN - *Virtual Private Network*), similare VLAN-urilor, dar care spre deosebire de acestea realizează criptarea informațiilor pentru o mai bună securizare a transmisiei.

VI.5 ECHIPAMENTE DE SECURIZARE (FIREWALL)

Internetul este o rețea cu foarte mulți utilizatori din întreaga lume și prin care se transferă cantități uriașe de informații.

Pentru aplicarea unei politici de securitate a rețelei, se utilizează echipamente de securizare de tip "zid de foc" (*firewall*) care aplică anumite reguli și constrângeri privind accesul pe diferite interfețe ale sale.

Un router poate fi configurat ca firewall. De asemenea, unele sisteme de operare (de exemplu, Windows XP) au opțiunea de activare a unui firewall intern.

Firewall-ul interconectează rețeaua publică și o rețea privată, asigurând securitatea datelor vehiculate intern în rețea și protecția rețelei private față de eventualele atacuri externe (Fig.VI.11).

Un firewall are minimum două interfețe:

- una pentru conexiunea dintre firewall și rețeaua publică (în particular, Internet-ul);
- cealaltă interconectează firewall-ul cu rețeaua internă privată (*intranet*), care necesită securizare.

Firewall-ul protejează rețeaua privată de unele atacuri externe și restricționează accesul din afară la resursele acesteia.

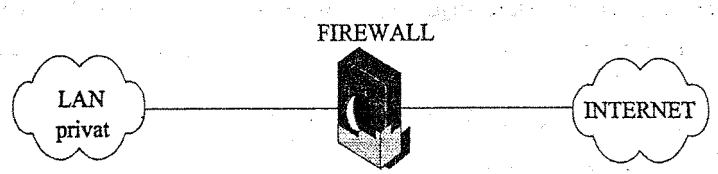


Fig. VI.11 Interconectarea unei rețele private cu una publică prin intermediul unui firewall

Întrucât firewall-ul reprezintă singura conexiune dintre rețeaua privată și cea publică, la nivelul său se poate monitoriza traficul de pachete și se verifică drepturile de acces ale utilizatorilor din afara rețelei interne (prin operația de *login*).

În prezent, se utilizează două tipuri de firewall:

1. **Poartă de aplicații** (*Application Gateway*) - varianta tradițională de firewall.

Orice conexiune între două rețele se face prin intermediul unui program de aplicații (*proxy*). O sesiune deschisă în rețeaua privată este încheiată de proxy, după care acesta creează o nouă sesiune spre nodul de destinație.

Programul proxy se bazează pe particularitățile suitei TCP/IP și este restrictiv pentru alte suite de protocoale. Execuția acestui program necesită resurse relativ mari din partea CPU.

La nivelul firewall-ului sunt admise numai acele protocoale pentru care sunt configurate aplicații proxy specifice. Cadrele bazate pe alte tipuri de protocoale sunt automat rejectate.

În practică, se configurează și firewall-uri transparente, care transferă cadrele între cele două sesiuni fără analiza prealabilă a datelor.

2. **Modul de inspecție dependent de stare** (*Stateful Inspection*) sau de **filtrare dinamică a pachetelor**, denumit și nod de control a accesului în funcție de context (CBAC - *Context-Based Access Control*) - concept relativ nou de implementare a firewall-ului.

În această tehnologie, se preiau pachetele de date și se citesc antetele introduse de protococolul de rețea (IP) și de cele corespunzătoare nivelelor OSI și TCP/IP superioare, până la nivelul de aplicație.

Firewall-ul verifică fiecare pachet care urmează să fie transferat și acordă dreptul de acces în funcție de adresele sursei și destinației, precum și de serviciul solicitat. Acest tip de firewall realizează controlul fluxului cu memorie, astfel încât echipamentul este capabil să recunoască acele pachete transmise din rețeaua publică (în particular, Internet) ca răspuns la o cerere adresată de un nod din rețeaua internă (*intranet*), prin monitorizarea sesiunilor TCP. În paralel, se rejectează toate pachetele transmise din rețeaua publică în cea internă, dar care nu provin din traficul inițiat intern.

Prin acest nou concept, se asigură o procesare rapidă și eficientă a traficului de informații dintre Internet și rețelele private, perfect adaptată noilor aplicații Internet și realizată cu resurse hardware relativ reduse.

Implementarea firewall-ului cu routere se face prin filtrarea dinamică a pachetelor și controlul traficului pe baza regulii care stabilește că:

- orice pachet transmis din rețeaua internă către o destinație externă este transferat de firewall necondiționat, cu excepția cazurilor în care se impun constrângeri;

- transferul oricărui pachet din rețeaua publică spre o destinație din rețeaua privată este blocat de firewall, cu excepția cazurilor în care se admite accesul acestora în mod explicit, prin configurarea adecvată a interfețelor publice referitor la accesul din exterior.

Interfețele firewall-ului sunt deschise numai pe durata sesiunii inițiate de un utilizator cu drept de acces.

Firewall-ul interceptează orice conexiune stabilită prin TCP și o continuă numai după verificarea prealabilă a legăturii.Acest lucru previne atacurile din exterior asupra rețelei private, prin distrugerea cadrelor transmise prin TCP fără drept de acces.

Firewall-ul poate fi configurat în vederea limitării accesului utilizatorilor din rețeaua internă în cea publică.

Mesajele generate prin ICMP pot fi transferate sau blocate de firewall în funcție de modul de configurare a acestuia.

Pentru evenimentele semnificative care apar la nivelul firewall-ului se pot trimite mesaje de înștiințare către nodurile de destinație accesate.

Echipamentele de tip firewall admit diverse protocoale de aplicație: FTP, NETBIOS, GRE, OSPF, RSVP (*ReSerVation Protocol*), VDOnet's VDOLive, Microsoft's NetShow etc.

Firewall-ul protejează rețeaua privată față de **atacurile externe** de tip "inundare" cu pachete (*flooding*), cu pachete PING ilegale sau ICMP generate în număr excesiv, atacuri
Smurf cu pachete având adresă IP din spațiul de adrese alocat rețelei private, de cele mai multe ori fiind chiar adresa de broadcast a acesteia, scanare a porturilor.

Firewall-ul permite controlul și monitorizarea accesului (*Logging Facility*) în rețeaua privată dar numai pentru sesiunile create pe baza protocolului Internet, nu și pentru alte suite de protocoale (Appletalk, DECnet, IPX/SPX).

Politica de securitate aplicată de firewall stabilește regulile pe baza cărora se admite sau se blochează transferul pachetelor între rețeaua privată și cea publică.

Un firewall devine activ numai după ce au fost configurate cel puțin o interfață publică și una privată și s-au stabilit regulile de acces la nivelul acestora.

Traficul între două interfețe ale firewall-ului nesupuse politicii de securitate se desfășoară normal, fără restricții.

Transferul pachetelor de la o interfață nesecurizată către una securizată este automat blocat.

Firewall-ul controlează traficul de pachete pe baza adreselor fizice sau IP, a porturilor de aplicație și chiar a zilei sau orei la care se accesează rețeaua.

Politica de securitate se aplică pe baza **listelor de acces** stocate în routere sau în servere RADIUS (*Remote Authentication Dial In User Service*).

RADIUS este un protocol de autentificare, configurare și contorizare a transferurilor între firewall, ca server de control a accesului (*Network Access Server*) și un server RADIUS care deține baza de date cu informații despre utilizatorii rețelei (nume de utilizatori și parole), modul de configurare a rețelei (adrese IP, măști de rețele și de subrețele etc), precum și despre sesiunile stabilite anterior, sub forma unui istoric al evenimentelor din rețea.

Firewall-ul este clientul RADIUS care adresează cererea de autentificare către serverele RADIUS, pentru accesarea listelor de acces. Acestea sunt fișiere de tip 'text' (.txt), codate ASCII, care includ liste de adrese IP sau MAC.

Listele de acces bazate pe adrese IP includ adrese IP individuale, eventual numele calculatoarelor-gazdă, domeniul de adrese IP al unei rețele și eventual unele comentarii care facilitează administrarea acestor liste.

Listele de acces cu adrese fizice includ adrese MAC individuale ale componentelor rețelei, eventual numele stațiilor și comentarii ajutătoare.

Numărul maxim de liste de acces care pot fi stocate pe un router precum și dimensiunile acestora este în general limitat.

Pentru un spațiu de adrese extins se preferă utilizarea unui server RADIUS care să gestioneze eficient aceste liste, pentru a reduce întârzierile de trafic produse de routere.

În acest caz, routerul devine un simplu client RADIUS care adresează cererea de autentificare către serverul RADIUS și primește un răspuns din partea acestuia.

Observații:

1. Filtrarea dinamică a pachetelor se realizează la nivelul firewall-ului prin politica de securitate dar și prin procedeele de translare a adreselor private în adrese publice (NAT; ENAT - *Enhanced NAT*). Pentru a evita dubla filtrare a pachetelor în routere, se dezactivează serviciul NAT pe durata activării firewall-ului.
2. Se poate monitoriza activitatea firewall-ului, mai precis evenimentele care se desfășoară la nivelul său:
   - accesarea adreselor de e-mail;
   - desfășurarea sesiunilor Telnet de acces de la distanță în rețeaua privată;
   - comunicarea pe porturi asincrone (de exemplu, interfețe seriale);
   - accesarea agenților SNMP.

VII

SERVICII ȘI TEHNOLOGII WAN

VII.1 SCHIMBUL DE CADRE (FRAME RELAY)

Schimbul de cadre (FR - *Frame Relay*) este un serviciu de rețea definit pentru comunicații rapide între routerele din WAN, realizate pe subnivelul inferior al nivelului OSI "legătură de date".

FR a fost standardizat de diferite organizații: CCITT(*Comitet Consultatif International de Telephonie et Telegraphy*) devenită ITU (*International Telecommunications Union*), ANSI (*American National Standardisation Institute*), ISO (*International Standards Organisation*) și altele.

Comunicația prin FR dintre routerele din WAN, văzute ca DTE-uri în rețeaua FR, se realizează pe conexiunile de date (DLC - *Data Link Connection*), definite pentru schimb de cadre (Fig. VII.1).

Una dintre legăturile DLC este rezervată pentru transmisia informațiilor de management dintre rutere și rețeaua FR, fiind denumită **interfață locală de management** (LMI - *Local Management Interface*).

Exceptând cadrele transmise prin LMI, toate celelalte sunt încapsulate în vederea transmisiei prin FR.

În antetul cadrului se include un câmp pentru identificatorul legăturii de date (DLCI - *DLC Identifier*) prin care routerul-sursă comunică cu cel de destinație.

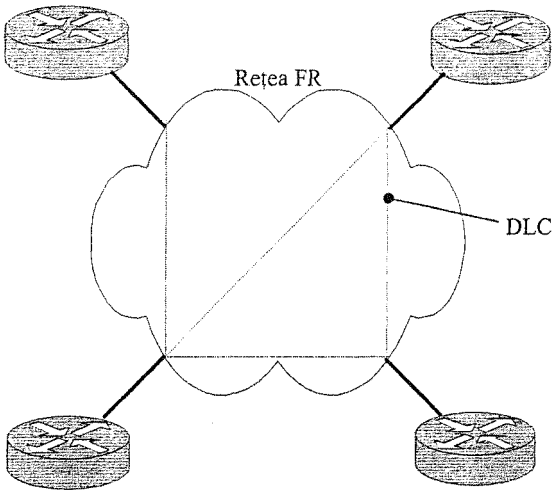


Fig.VII.1 Conexiuni pentru FR

Lungimea acestui câmp depinde de modul de implementare a rețelei FR.

Într-un câmp suplimentar se poate specifica tipul protocolului de rețea utilizat pentru transmisie, în cazul în care comunicația se desfășoară între routere multiprotocol (RFC 1294).

Observații:

1. Serviciul FR nu efectuează controlul erorilor de transmisie ceea ce permite comunicația la viteze foarte mari.
2. Conexiunile dintre routere prin FR pot fi realizate pe linii sincrone prin intermediul unor interfețe de mare viteză (X.21, V.35), pe linii comutate cu legături ISDN sau în sisteme cu acces mutiplu, cu mutiplexare în timp (TDM - *Time Division Multiplexing*), conform standardului G.703.
3. Prin configurarea adecvată a rețelei FR, se pot realiza și transmisii de tip broadcast sau multicast.

VII.1.1 ÎNCAPSULAREA FRAME RELAY

S-au propus mai multe standarde pentru încapsularea datelor în rețelele FR.

Aceasta se poate face asemănător specificațiilor protocolului HDLC (*High-level Data Link Control*), în cadre delimitate de caractere speciale (*flags*) care se transmit pe linie și pe durata

pauzelor, cu un câmp de adrese de 2-4 octeți (B - *Byte*) și unul de control (1-2 octeți), urmate de câmpul datelor (Fig.VII.2).

Flag 1B	Câmp de adrese 2B - 4 B	Câmp de control 1B - 2B	Câmpul datelor	Flag 1B

Fig. VII.2 Formatul standard al cadrului HDLC

Standardul referitor la încapsularea FR, definit de IETF (*Internet Engineering Task Force*) în RFC 1490, completează cadrul HDLC cu un câmp de un octet care identifică protocolul de rețea utilizat pentru transmisie (NLPID - *Network Layer Protocol IDentifier*) și un câmp suplimentar, cu valori tipice dependente de protocol (Fig. VII.3).

Flag 1B	DLCI 2B - 4B	Câmp de control 2B *	NLPID 1B	Câmp suplimentar ≤ 5B	DATE	Flag 1B

Fig. VII.3 Formatul cadrului FR-HDLC definit de RFC 1490

Câteva valori și semnificații ale câmpului NLPID și conținutul câmpului suplimentar sunt prezentate în tabelul VII.1.

Tabel VII.1

Valori ale câmpului NLPID și ale celui suplimentar

din cadrul FR-HDLC conform RFC 1490

Câmp NLPID		Câmp suplimentar	
Valoare înscrisă	Semnificație	Valoare înscrisă	Semnificație
0x.80	Câmpul suplimentar de 5 octeți specifică tipul protocolului în format SNAP (*SubNetwork Access Protocol*)	0x.00.00.00.08.06	ARP
		0x.00.00.00.81.37	IPX
		0x.00.08.C2.00.0E	STA
0x.CE	Câmpul suplimentar de 2 octeți specifică tipul cadrului Ethernet, dependent de protocolul de rețea	0x.08.00	IP
		0x.08.06	ARP
		0x.81.37	IPX
0x.CC	Se utilizează pentru transmisie protocolul Internet	nu există	

Formatul cadrului FR-HDLC definit pentru echipamente CISCO (Fig. VII.4) este modificat față de cel definit prin RFC 1490, prin excluderea câmpului de control.

Flag 1B	DLCI 2B - 4B	Tipul cadrului Ethernet 2B	DATE	Flag 1B

Fig. VII.4 Formatul cadrului FR-HDLC definit de CISCO

VII.1.2 IDENTIFICAREA CONEXIUNILOR FRAME RELAY

Într-o rețea FR, pentru fiecare router sunt configurate câteva legături de date (DLC) cu alte routere din rețea.

Comunicația dintre routere se realizează prin schimb de cadre pe una din legăturile active, specificată în fiecare cadru transmis prin identificatorul legăturii (DLCI).

Identificatorii de conexiune au semnificații locale la nivelul fiecărui router.

Rețeaua FR preia cadrul transmis de routerul-sursă, interpretează câmpul DLCI definit de acesta și îl modifică corespunzător routerului-destinație.

Alocarea acestor identificatori (DLCI) se poate face aleator sau sistematic, cu identificarea unică a routerului de destinație (Fig. VII.5).

VII.1.3 GESTIONAREA REȚELELOR FRAME RELAY

Gestionarea resurselor rețelelor FR se realizează prin transmisia informațiilor de management între fiecare router și rețeaua de comutație FR.

Periodic routerele interoghează rețeaua și primesc prin interfața locală de management (LMI) informații referitoare la legăturile de date (DLC) active, realocate sau nou configurate.

Interfața de management este asociată unei conexiuni de date cu identificator prestabilit. De exemplu, în standardele ANSI și Q.933 se utilizează DLCI = 0. Conform standardelor consorțiului producătorilor de echipamente, se impune DLCI = 1023.

Procesul de management se completează prin transmisia periodică a informațiilor referitoare la starea fiecărui router către rețea.

În rețelele FR cu configurare statică a conexiunilor DLC, nu se utilizează LMI. Conexiunile sunt activate sau dezactivate prin comenzi de configurare de tip "adăugare" (*add*) sau de "eliminare" (*remove*).

Routerele sunt informate prin LMI ori de câte ori se activează sau se dezactivează o conexiune DLC din cadrul unei interfețe FR.

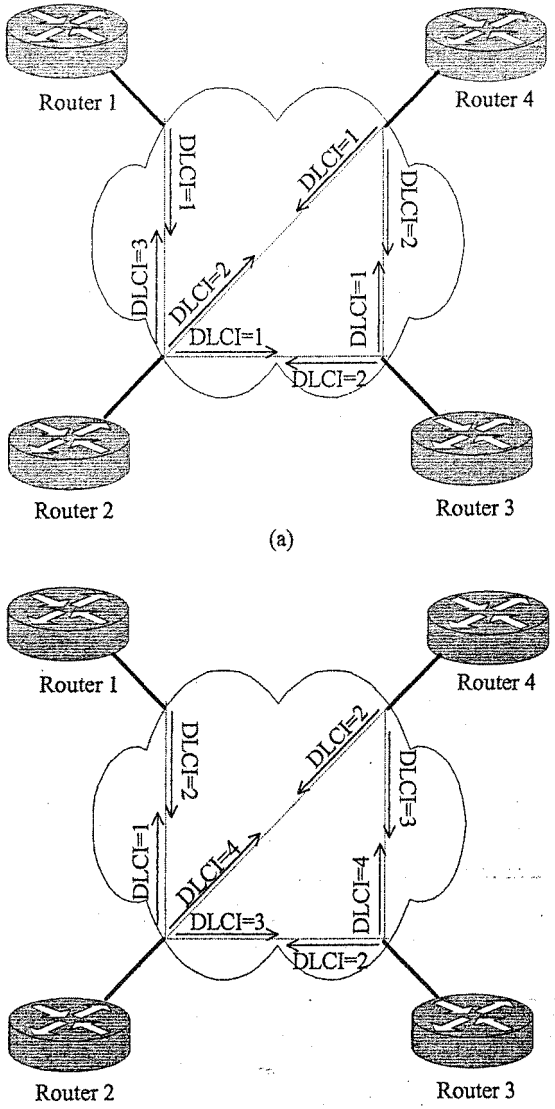


Fig. VII.5 Asocierea valorilor DLCI cu conexiunile DLC
(a) aleator; (b) sistematic.

Operațiile de activare (*enable*), dezactivare (*disable*) sau de reinițializare (*reset*) a unei legături de date (DLC) se realizează prin comenzi specifice programelor software de configurare, în care se specifică identificatorul de conexiune (DLCI).

VII.1.4 INTERFEȚE FRAME RELAY

În rețelele FR, procesele de comunicație se realizează la nivel fizic prin **interfețele fizice** FR (FRI - *Frame Relay Interface*) iar între nivelele OSI superioare, prin **interfețele logice FR** (FRLI - *Frame Relay Logical Interface*), configurate la nivelul celor fizice.

Fiecare FRLI include un subset de conexiuni DLC disponibile la nivelul unei interfețe fizice.

Implicit, FRLI 0 se definește pentru fiecare interfață fizică FR și include toate conexiunile DLC create pe aceasta.

Dacă o interfață FRLI este asociată unei singure conexiuni DLC, atunci ea este creată pe principiul comunicației punct-la-punct (PTP - *Point-To-Point*).

Interfețele FRLI cu conexiuni DLC multiple se configurează ca interfețe cu acces multiplu fără difuzare (NBMA - *Non-Broadcast Multiple Access*).

Când o interfață FR este **dezactivată** (*disable*), procesul LMI este întrerupt și pe toate conexiunile stabilite pe acea interfață se transmite un mesaj de eroare (*fault*). Interfața FR poate fi **reactivată** prin comanda de activare (*enable*).

Reinițializarea unei interfețe FR (*reset*) are ca efect eliminarea tuturor conexiunilor DLC existente în lista de legături de date a interfeței și informarea prin LMI a tuturor routerelor din rețea de pierderea acestor legături. Informațiile referitoare la legăturile DLC configurate anterior procesului de resetare a interfeței sunt stocate în baza de date de management a rețelei FR și se transmit prin LMI către routere atunci când se reactivează interfața.

VII.1.5 CONGESTIA REȚELELOR FRAME RELAY

Transmisia datelor pe principiul FR se face în regim normal la viteze foarte mari, ceea ce poate determina supraîncărcarea echipamentelor și apariția congestiilor în trafic. Din acest motiv, activarea serviciului FR se face printr-un mecanism de creștere treptată, controlată a vitezei de transmisie, de la valori foarte mici către valori tot mai mari, cu un anumit factor de creștere (k_i).

Este importantă adaptarea vitezei de transmisie în rețeaua FR la viteza de transfer a pachetelor de date de pe nivelele OSI superioare către interfețele FR, pentru a reduce lungimea "cozilor de așteptare" și pentru a evita depășirea capacității de stocare a bufferelor, urmată de pierderea datelor.

Pe aceste considerente se poate decide scăderea vitezei de transmisie prin FR, cu un anumit factor de descreștere (k_d).

Viteza de transmisie a datelor în rețele FR este limitată de:

- lățimea de bandă (B) a interfeței FR;
- viteza de comunicație dintre interfața FR și nivelele OSI superioare;
- apariția congestiilor în traficul rețelei FR.

Furnizorul de serviciu FR garantează o anumită viteză medie de transfer a datelor în rețeaua FR, în regim normal de funcționare (CIR - *Committed Information Rate*).

Depășirea vitezei medii (CIR) și transmisia cu o rată mai mare (DIR - *Desired Information Rate*) pot determina aglomerarea rețelei cu cadre, saturarea bufferelor și **congestia** rețelei FR.

În figura VII.6, este reprezentată grafic evoluția vitezei de transmisie într-o rețea FR.

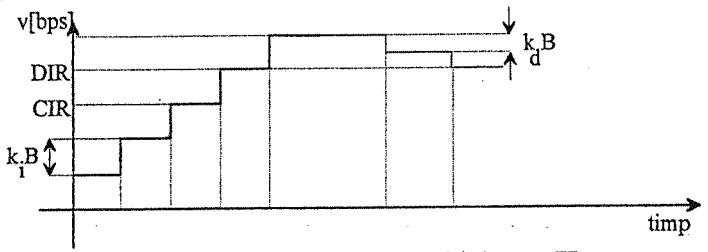


Fig. VII.6 Graficul vitezei de transmisie în rețea FR

La apariția unei congestii de trafic, routerul respectiv este informat prin intermediul interfeței de management a rețelei urmând ca acesta să-și reducă viteza de transmisie a datelor în rețea.

Informarea routerelor se poate face în două moduri:

- prin **mesaje CLLM** (*Consolidated Link Layer Management*) transmise pe conexiunea cu identificator DLCI = 1007 (stabilit prin standardul Q.933), mesaje de avertizare care se transmit în mod repetat până la soluționarea congestiei;
- prin **setarea bitului BECN** (*Backward Explicit Congestion Notification*) inclus în fiecare cadru de date. Routerele testează acest bit și la detecția unui bit BECN cu valoare logică '1' se ia în

considerare iminența producerii unei congestii în rețeaua FR, ceea ce determină limitarea vitezei de transmisie a routerului la valoarea medie CIR. În continuare, routerul contorizează biții succesivi BECN cu valoare '1' și dacă numărul acestora depășește o valoare maxim admisă (BECNLIMIT), atunci se reduce treptat rata de transmisie, la 0,625 CIR, 0,5 CIR, 0,25 și așa mai departe până la normalizarea traficului. În următoarea perioadă de timp, creșterea vitezei se face treptat, cu un factor de creștere mic, pentru evitarea reapariției congestiei. Dacă riscul de congestie devine nul, se reia transmisia cu viteză medie CIR și chiar DIR.

Evoluția vitezei de transmisie a datelor la nivelul unei interfețe FR, în cazul apariției unei congestii, este reprezentată grafic în figura VII.7.

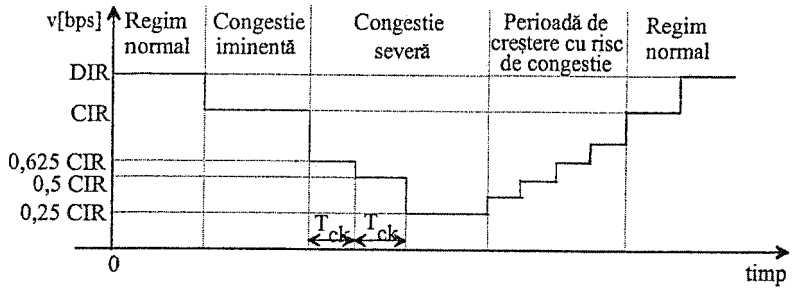


Fig. VII.7 Graficul vitezei de transmisie în caz de congestie într-o rețea FR

Observație:

Comunicația dintre routere în rețele FR se poate face cu compresie și/sau criptare a datelor (ENCO - *ENcryption / COmpression*). Routerele negociază aplicarea acestor procedee de transmisie (RFC 1962; RFC 1968) și după aceea se activează conexiunea DLC pentru schimbul de cadre. Dacă routerul-destinație nu are implementat mecanismul de decriptare, legătura DLC cu criptare devine inutilizabilă. Algoritmii de compresie sunt în general incluși în pachetul software aferent routerului. Algoritmii de criptare sunt opționali. În cazul în care nu sunt implementați pe router, se poate utiliza o cartelă de criptare (MAC - *MiniAccelerator Card*).

VII.2 TRANSMISIA VOCII ÎN PACHETE (VoP)

Rețelele de calculatoare furnizează diferite servicii de rețea și aplicații diverse.

Pe lângă transferul de date, un rol aparte în rețea îl au aplicațiile în timp real, cu transmisii vocale, audio sau video, pe baza protocolului RTP (*Real-Time Protocol*).

Integrarea fluxului vocal cu cel de date în rețelele de calculatoare existente (IP, ATM, FR etc), crește gradul de atractivitate al acestora, durata de accesare a lor, precum și numărul de utilizatori.

Transmisia vocii în pachete (VoP - *Voice over Packet*) reprezintă un serviciu de rețea diferit de transmisia datelor, care se poate efectua simultan cu aceasta.

Calitatea vocii transmise este foarte bună în rețelele ATM datorită lungimii mici a celulelor ATM care reduc întârzierile de transmisie, dar mai slabă în rețelele IP. De aceea, s-a propus transferul fluxului IP printr-o rețea de transport ATM (*IP-over-ATM*).

Calitatea serviciului de voce (QoS - *Quality of Service*) oferit de o rețea IP se poate îmbunătăți prin aplicarea protocolului RSVP și a tehnologiei MPLS (*MultiProtocol Label Switching*).

Spre deosebire de rețeaua de telefonie publică (PSTN - *Public Switching Telephony Network*) care transmite vocea prin intermediul circuitelor de comutare, rețelele LAN și WAN realizează transmisiile vocale în rețea (VoN - *Voice over Network*) prin **comutare de pachete,** fiind denumite și **rețele de transfer a pachetelor** (*Packet Network*).

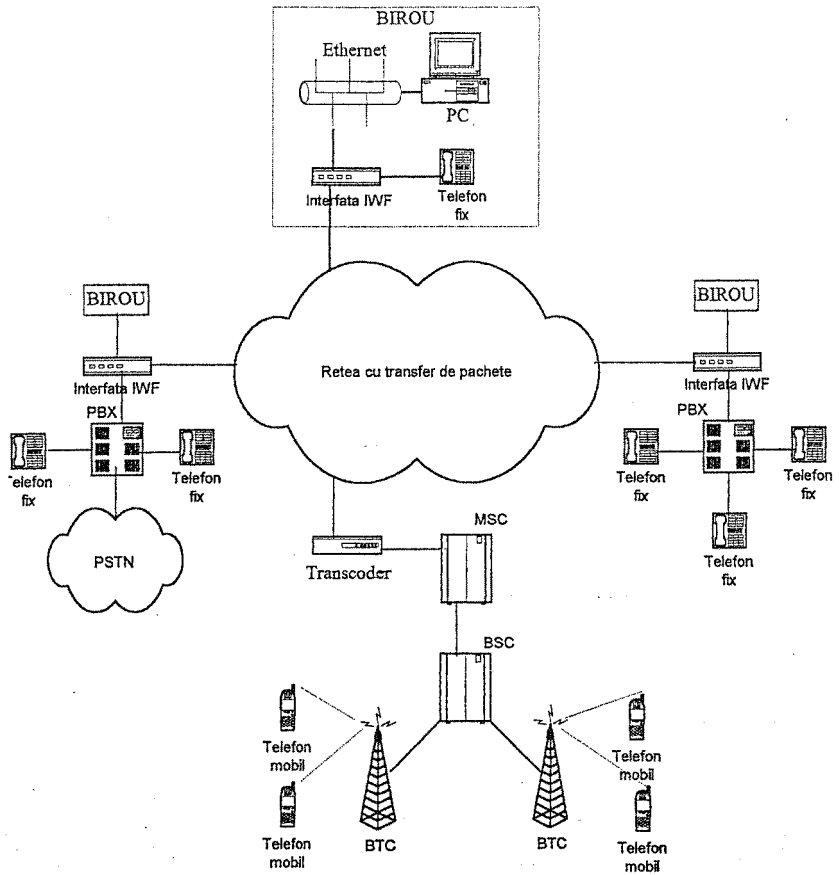
VII.2.1 INTEROPERABILITATEA SERVICIULUI VoP

Serviciul de transmisie a vocii în pachete (VoP), poate fi implementat în diferite rețele, cu diverse tehnologii:

- VoIP (*Voice-over-Internet Protocol*) în rețele IP;
- VoATM (*Voice-over-ATM*) sau VToA (*Voice-To-ATM*) în rețele ATM;
- VoFR (*Voice-over-Frame Relay*) în rețele FR;
- VoDSL (*Voice-over-Digital Subscriber Line*), pe liniile digitale de abonat.

Pentru ca o rețea cu transfer de pachete să transporte și voce, și date, este necesară implementarea **funcției de interoperabilitate** (IWF - *Interworking Function*), atât din punct de vedere fizic (*hardware*), cât și din cel al algoritmilor software.

Pentru interconectarea cu rețelele de telefonie celulară, interfețele IWF trebuie să realizeze suplimentar, conversia de format a pachetelor (*transcoding*) între rețeaua de calculatoare și cea de comunicații mobile (Fig.VII.8). În sistemele telefonice celulare, vocea este digitizată, compresată și transmisă în pachete cu format specific. Transferul vocii în rețelele de calculatoare este posibilă numai prin extragerea datelor din pachetele generate în sistemul celular și reîncapsularea lor în formatul propriu rețelei de transfer a pachetelor.



MSC - Mobile Switching Center
BSC - Base Station Controller
BTC - Basic Transceiver

Fig.VII.8 Exemplificarea unei rețele cu VoP

Interfețele IWF pentru conectarea la rețeaua de calculatoare a aparatelor telefonice se implementează în variantă analogică.

La aceeași rețea se pot conecta și centrale telefonice private (PBX - *Private Branch Exchange*), prin intermediul unor interfețe IWF care implementează algoritmii software de semnalizare și care, printr-un circuit de emulare, pot transmite și în rețeaua telefonică publică.

Prin rețeaua de transfer a pachetelor se pot interconecta mai multe centrale telefonice private, pentru transferul "trunchiurilor" de convorbire între centrale (*trunking*). În acest caz, interfețele IWF trebuie să aibă capacități mari de transmisie (de exemplu, flux E1 de 2,048 Mbps sau T1 de 1,544 Mbps).

VII.2.2 CALITATEA SERVICIULUI DE VOCE

Transmisia vocii în rețele cu transfer de pachete este avantajoasă prin costurile reduse și lățimea de bandă mică utilizată pentru serviciul VoP.

Totuși, în procesul de transmisie a vocii în rețele de calculatoare simultan cu datele, apar anumite aspecte nedorite care afectează calitatea semnalului transmis.

De aceea, se utilizează un indice de calitate a serviciului (QoS) pentru aprecierea performanțelor transmisiei vocale în rețelele de calculatoare.

Reflexiile de semnal în secțiunile cu dezadaptare de impedanță din rețea și întârzierile de propagare de peste 50 ms creează **fenomenul de ecou** și este necesară utilizarea unor circuite de suprimare a ecourilor.

Suprapunerea semnalelor de convorbire (*Talker Overlap*) de la cele două capete devine deranjantă pentru întârzieri mai mari de 250 ms.

Întârzierile de transmisie sunt cauzate de diferiți factori:

- codarea vocii (*vocoding*) se realizează pe principiul codării-bloc ceea ce impune stocarea eșantioanelor de voce în memorii-tampon (*buffer*) în vederea formării unui bloc de intrare (Tabel VII.2);
- împachetarea biților rezultați din codarea vocii în pachete de anumite dimensiuni cu scopul reducerii ponderii antetelor și a încărcării rețelei (de exemplu, trei cadre G.729 corespunzând la 30 ms de convorbire se pot transmite într-un singur pachet);
- fenomenul de propagare pe linie (*end-to-end delay*);
- procesul de refacere a mesajului prin reordonarea fragmentelor transmise în cadre și/sau pachete multiple, eventual pe căi diferite din rețea;

• procesul de sincronizare pentru eliminarea erorilor de stabilire a momentelor optime de eșantionare a semnalului recepționat (*jitter*).

Pierderea unor pachete este un fenomen critic pentru rețelele IP, fiind necesară compensarea lor prin interpolarea secvenței sau prin transmisia redundantă a pachetelor de voce, cu un excedent de bandă compensabil prin scăderea ratei vocoderului și cu întârzieri suplimentare de transmisie.

Tabel VII.2

Standarde pentru vocodere cu compresie

Standard	Descriere	Viteza de transmisie (kbps)	Durata blocului de intrare (ms)
G.726	ADPCM (*Adaptive Differential Pulse Code Modulation*)	16; 24; 32; 40	0,125
G.728	CELP (*Code Excited Linear Prediction*)	16	2,5
G.729	ACELP (*Adaptive Code Excited Linear Prediction*)	8	10
G.723	MRC (*MultiRate Coder*)	5,3 și 6,3	30

Observație:

Standardul G.711 descrie transmisia digitală a vocii fără compresie, cu codare în sistem PCM (*Pulse Coded Modulation*), cu viteză de 64 kbps.

VII.2.3 ARHITECTURA SISTEMULUI VoIP

Conectarea aparatelor și centralelor telefonice la o rețea de calculatoare impune tranferul semnalelor de convorbire și al celor de semnalizare precum și adaptarea formatului acestora la rețeaua de transmisie a vocii.

Sistemul VoIP include patru module software (Fig. VII.9):

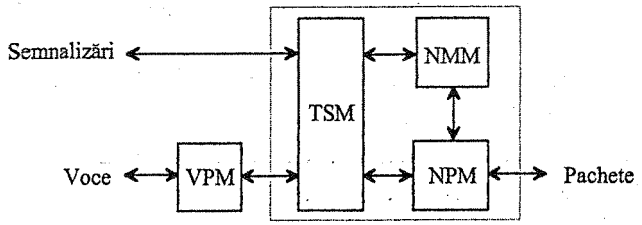


Fig. VII.9 Arhitectura sistemului VoIP

1. **Modulul de procesare a vocii și pachetelor vocale** (VPM - *Voice Packet Module*) convertește eșantioanele de voce în pachete generice și invers. Suplimentar, acest modul, implementat cu un procesor digital de semnal (DSP - *Digital Signal Processing*), cu interfață PCM, efectuează operații de suprimare ecourilor (G.165) pentru transmisii duplex, compresie a vocii prin detecția perioadelor de activitate vocală și suprimarea perioadelor de "liniște", generare a tonului (DTMF - *Dual Tone MultiFrequency*), diferențierea pachetelor de voce și fax, eliminarea jitterului, sincronizarea de bit și de cadru, reordonarea fragmentelor din pachetele recepționate, redarea vocii în mod continuu din eșantioanele stocate în buffere de tip FIFO (*First In, First Out*).

2. **Modulul de semnalizări telefonice** (TSM - *Telephony Signaling Module*) interpretează semnalizările de pe linia telefonică (de exemplu, semnalizări SS7 - *Signaling System 7*) relativ la schimbările stării sistemului.

3. **Modulul protocolului de rețea** (NPM - *Network Protocol Module*) configurează conexiunile în rețea pe baza comenzilor date de TSM, formează pachetele de voce și de semnalizare cu antete specifice dependente de protocol. Semnalizarea în rețeaua de calculatoare se realizează pe baza diferitelor standarde, de exemplu Q.933 pentru semnalizări în sisteme VoFR.

4. **Modulul de management** a rețelei (NMM - *Network Management Module*) gestionează resursele sistemului VoIP, conform standardului (ANSI).1 compatibil cu (SNMP).V1 sau conform unor standarde de firmă.

Modulele TSM, NMM și NPM sunt implementate cu un microprocesor.

Observații:

1. Serviciul VoIP nu se reduce numai la transmisii de voce și fax (V/FoIP - *Voice/Fax over IP*) ci se extinde și la aplicațiile multimedia, de exemplu conferințe on-line cu mai mulți utilizatori.

2. În numeroase cazuri, serviciul VoIP este implementat cu rețea de transport ATM, pentru creșterea calității transmisiei.

VII.2.4 CARACTERISTICILE SERVICIULUI VoATM

Serviciul VoATM a fost proiectat de la început ca tehnologie multimedia, cu servicii multiple (*multiservice*), de viteză ridicată.

Rețeaua ATM folosește circuite de emulare (CES - *Circuit Emulation Service*) pentru a transporta traficul din alte rețele (IP, E1, T1 etc).

În sistemele ATM, semnalul vocal este interpretat ca o succesiune de intervale de convorbire (*bursts of speech*) și de "liniște" (*silence*), iar vocoderul îl procesează cu o rată de codare constantă (CBR - *Constant Bit Rate*) ceea ce determină creșterea complexității serviciului VoP.

Forumul VoATM și ITU au propus diferite standarde pentru transmisia vocii și a trunchiurilor de convorbire (*trunking*) în rețele ATM (Tabel VII.3).

Tabel VII.3

Standarde VoATM

Standard	Compresia vocii	Rejectarea pauzelor	Utilizarea concentratoarelor
CES	-	-	-
AAL-1 (*trunking*)	-	-	✓
VoIP over ATM	✓	✓	-
AAL-2 (*trunking*)	✓	✓	✓

VII.2.5 ECHIPAMENTE DE TRANSMISIE VoP

Pentru transportul vocii în rețelele de calculatoare sunt necesare echipamente de comutație cu arhitectură distribuită denumite **porți de mediu** (MG - *Media Gateway*), cu număr foarte mare de porturi de utilizator (de ordinul sutelor de mii), în fiecare nod al rețelei. Aceasta reprezintă caracteristica de **scalabilitate** a porții de mediu. MG este responsabil de comutarea între rețeaua de date și cea de voce, de adaptarea semnalului vocal pentru transferul în pachete (digitizare, compresie, suprimarea ecourilor, împachetare).

Un MG funcționează conform unui protocol de control Megaco sau MGCP (*Media Gateway Control Protocol*), implementat în controlerul porții de aplicație, denumit și **comutator logic** (*softswitch*). Prin urmare, MG este un echipament **controlabil.**

MG trebuie să aibă interfețe de acces în diverse rețele (cu transmisie pe cablu, fibră optică sau "fără fir") și să permită comutarea între rețele diferite (IP, ATM, FR, DSL, TDM), aceasta fiind caracteristica de **interoperabilitate** a porților de mediu.

De asemenea, ca un indice de performanță a transmisiei, se impune o perioadă minimă de bună-funcționare de 99,999 % din durata totală de funcționare ("regula celor cinci de nouă").

MG poate interconecta diferite tehnologii de transmisie a vocii:

- TDM (*Time Division Multiplexing*) - metoda tradițională cu circuite de comutare;
- ATM AAL-1/AAL-2;

- IP pur sau cu rețea de transport ATM, pe baza protocoalelor RTP și RTCP (*Real Time Control Protocol*).

Pentru semnalizarea în rețea, se utilizează o **poartă de aplicații de semnalizări** (SG - *Signaling Gateway*) care interfațează sistemul telefonic de semnalizare (SS7) cu rețeaua de transport VoP.

Compatibilitatea cu sistemul telefonic actual este asigurată de un **server de aplicație** care adaptează semnalul transmis la serviciile telefonice standard de clasă 4 și clasă 5.

În concluzie, serviciul de transmisie a vocii în pachete (VoP), se poate implementa în diferite sisteme (VoIP bazat pe MPLS, VoATM etc), compatibile cu rețelele telefonice existente de tip TDM și cu cele de transport a datelor (IP, ATM, FR, DSL etc), pe baza standardelor organizațiilor acreditate, folosind diverse echipamente cu performanțe apreciate prin indicele de calitate a serviciului QoS și prin alți indici de evaluare a calității semnalului vocal recepționat.

VII.3 ISDN

Rețeaua digitală cu servicii integrate (ISDN - *Integrated Services Digital Network*) este definită de ITU-T într-o serie de recomandări, ca serviciu oferit în WAN pentru transportul fluxului din rețelele IsoEthernet, principiile de bază ISDN fiind expuse în recomandarea I.120 din 1988. Conform acesteia, ISDN oferă în aceeași rețea, servicii simultane de voce și date. ISDN se poate implementa fie în rețele digitale cu circuite de comutație, fie în cele cu comutare de pachete, fie în structuri fără comutație, cu circuite alocate semipermanent.

Elementul fundamental al ISDN este **calea primară** de 64 kbps.

Accesul clienților la rețeaua ISDN se poate realiza prin diferite metode, dintre care cele mai utilizate sunt:

1. **BRA** (*Basic Rate Access*) - cu două canale B de 64 kbps și un canal D de 16 kbps.
2. **PRA** (*Primary Rate Access*) - cu până la 30 de canale B de 64 kbps și un canal D de 64 kbps.

Canalele ISDN de tip B (*B channel*) sunt canale alocate utilizatorilor, pentru transport de date, voce codată PCM, eventual fluxuri de date provenind de la mai multe surse cu debite informaționale relativ mici, mixate.

Toate fluxurile informaționale care se transferă pe un anumit canal B au aceeași destinație, dar fiecare canal B poate avea o destinație diferită de a celorlalte canale.

Pe un canal B se pot stabili trei tipuri de conexiuni:

- cu circuite de comutație, semnalizările fiind transmise pe canalul adiacent de tip D.

• cu comutare de pachete, conform standardului X.25 al CCITT.

• semipermanentă, oferită de furnizorul de servicii ISDN.

Canalele ISDN de tip D sunt utilizate fie pentru semnalizări, fie pentru comutare de pachete cu viteze mici.

VII.3.1 INTERFEȚE BRI

O conexiune ISDN prin metoda BRA se realizează conform schemei din figura VII.10.

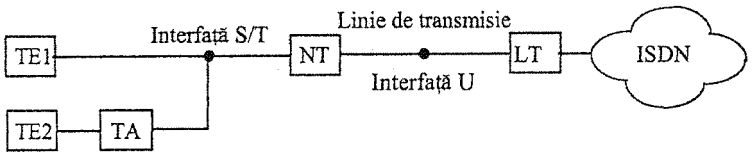


Fig. VII.10 Schemă de conexiuni BRA

Routerele prevăzute cu interfețe BRI (*Basic Rate Interface*) sunt considerate, în rețeaua ISDN, **echipamente terminale de tip 1** (TE1 - *Terminal Equipment 1*).

Routerele care nu sunt direct compatibile ISDN sunt considerate **echipamente terminale de tip 2** (TE2 - *Terminal Equipment 2*).și necesită un **adaptor de terminal** (TA - *Terminal Adapter*) pentru conectare la rețeaua ISDN.

Mai multe echipamente TE1 și/sau TE2 împart resursele (*sharing*) unei linii S/T (recomandarea ITU-T I.430) de lungime limitată și se conectează la un bloc unic de terminație de rețea (NT - *Network Termination*), separat sau integrat în echipamentul utilizatorului (standard ANSI T1.601-1992).

Interfața BRI folosește o conexiune de tip 'magistrală' (*bus*) care permite accesul multiplu pe linia S/T, mai precis accesul mai multor echipamente de utilizator (routere, telefoane etc), adresate prin **identificatori de terminal** (TEI - *Terminal Endpoint Identifier*).

Comunicația dintre terminația de rețea NT și cea de linie LT (*Line Termination*) se realizează pe o linie de transmisie care poate avea lungimi de ordinul kilometrilor.

Interfața U se utilizează numai dacă terminația NT este inclusă în blocul utilizatorului (valabil în Statele Unite ale Americii).

Conectarea unui TE la bucla S/T se face cu conectori RJ-45 cu 8 pini care asigură atât transmisia și recepția datelor, cât și alimentarea circuitelor.

TE și NT comunică prin cadre de 48 de biți, cu durata de 250 ms, care transportă 4 biți de pe canalul D și câte 16 biți de pe fiecare canal B.

Viteza de transmisie globală prin metoda BRA, cu canale 2B+D, nu este de numai 144 kbps corespunzător debitelor canalelor, ci de 192 kbps, deoarece în cadrele transmise se adaugă antete și câmpuri de sincronizare.

Pe canale suplimentare de 80 bps (cinci canale S dinspre NT spre TE și un canal Q pentru comunicația în sens invers), se transmite informația de sincronizare în mai multe cadre, operație denumită **transmisie de cadre multiple** (*multiframing*).

Observații

1. Trebuie făcută distincția între cadrele folosite pentru comunicația dintre un TE și NT și cadrele transmise pe linia S/T, conform protocolului HDLC.

2. Protocolul ISDN prevede alocarea la nivelul terminației de rețea a unui canal B pentru un singur TE la un moment dat. Această constrângere permite evitarea coliziunilor în circuitul S/T. Dar această problemă nu este soluționată la nivelul TE, fiind necesară implementarea unui mecanism pentru evitarea coliziunilor, capabil să detecteze o coliziune, să finalizeze transmisia pentru unul dintre echipamentele TE implicate în coliziune și să aplice o schemă de priorități dinamică. Prioritatea unui TE este minimă imediat după încheierea unei transmisii și crește pe durata intervalului de așteptare. Informațiile de semnalizare au prioritate maximă.

Între NT și LT, datele se transmit în cadre de 240 de biți, cu durata de 1,5 ms. Un astfel de cadru include câte 96 de biți de pe fiecare canal B, 24 de biți de pe canalul D și biți suplimentari de sincronizare, detecție de erori (cu polinoame CRC), de control a stării interfețelor etc.

Interfața BRI a ruterului funcționează conform modelului OSI pe mai multe nivele.

Modulul software corespunzător nivelului fizic (*Layer 1*) al interfeței nu necesită în regim normal ISDN configurări speciale din partea utilizatorului, ci numai dacă se folosesc conexiuni semipermanente, cu multiplexare în timp (TDM - *Time Division Multiplexing*).

Pentru nivelul legăturii de date (*Layer 2*) se poate atașa un modul software care implementează un protocol de comunicație de nivel OSI 2 (de exemplu, PPP - *Point-to-Point Protocol*), adecvat configurat pentru alocarea unui canal B denumit și **slot ISDN** (B1 sau B2) din canalul ISDN BRA. Transmisia datelor pe acest nivel al BRI se face conform protocolului HDLC.

VII.3.2 INTERFEȚE PRI

Pentru comunicații în rețeaua ISDN cu viteze superioare celor oferite de metoda BRA, se utilizează o structură de canale ISDN definită de metoda PRA, în două variante:

• 2048 kbps - interfață E1 cu 30 de canale B și un canal D de 64 kbps (utilizată în Europa,

Australia și Noua Zeelandă);

- 1544 kbps - interfață T1 cu 23 de canale B și un canal D (utilizată în S.U.A și Japonia).

Schema de conexiuni PRA este prezentată în figura VII.11.

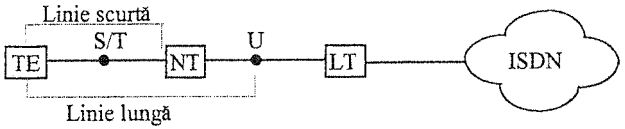


Fig.VII.11 Schemă de conexiuni PRA

Routerul TE comunică în rețeaua ISDN prin interfața PRI (*Primary Rate Interface*) de tip E1, cu NT separat și linie S/T scurtă (maximum 200 metri), sau de tip T1, cu NT inclus în echipamentul utilizatorului și linie S/T lungă (maximum 1800 metri) conform recomandărilor ITU-T I.411 și I.431.

Conexiunea dintre TE și NT este de tip 'punct-la-punct' și nu admite accesul multiplu. Doar un singur echipament terminal se poate conecta la o interfață PRI. Caracteristicile fizice și electrice ale conexiunii sunt prezentate în recomandarea ITU-T G.703 (cablu coaxial de 75 Ohmi sau cablu simetric în perechi de 120 Ohmi).

Comunicația dintre TE și NT se face prin cadre de 256 de biți, cu 32 de intervale (sloturi) de 8 biți.

Slotul 0 este rezervat pentru transmisia informațiilor de sincronizare și încapsulare iar slotul 16 este alocat canalului D. Numai 30 de sloturi sunt oferite utilizatorilor pentru comunicații în rețeaua ISDN.

Dacă interfața PRI nu este utilizată pentru aplicații ISDN, atunci slotul 16 nu mai este rezervat și se oferă utilizatorului un canal dedicat de 2 Mbps, mai precis cu un flux de 1984 kbps, corespunzător celor 31 de sloturi. Slotul 0 este în continuare rezervat.

Deci, primii 8 biți ai fiecărui cadru sunt rezervați și au semnificații distincte, repetitive pe mai multe cadre (*multiframing*), conform Tabelului VII.4. Un cadru multiplu este format din 16 cadre succesive.

Conexiunea PRA are trei stări posibile:

1. pauză de transmisie (*no signal*).
2. regim normal de transmisie
3. regim de alarmare, pe durata căruia NT transmite unui TE un semnal de alarmă AIS (*Alarm Indication Signal*) atunci când apar erori în rețeaua ISDN și sunt afectate datele recepționate de NT având ca destinație acel TE.

Tabel VII.4

Semnificațiile și valorile biților din sloturile 0
ale unui cadru multiplu transmis prin PRI

	Subcadru multiplu	Numărul cadrului	Numărul de ordine al bitului							
			1	2	3	4	5	6	7	8
Cadru multiplu	I	0	C1	0	0	1	1	0	1	1
		1	0	1	A	S4	S5	S6	S7	S8
		2	C2	0	0	1	1	0	1	1
		3	0	1	A	S4	S5	S6	S7	S8
		4	C3	0	0	1	1	0	1	1
		5	0	1	A	S4	S5	S6	S7	S8
		6	C4	0	0	1	1	0	1	1
		7	0	1	A	S4	S5	S6	S7	S8
	II	8	C1	0	0	1	1	0	1	1
		9	1	1	A	S4	S5	S6	S7	S8
		10	C2	0	0	1	1	0	1	1
		11	1	1	A	S4	S5	S6	S7	S8
		12	C3	0	0	1	1	0	1	1
		13	E	1	A	S4	S5	S6	S7	S8
		14	C4	0	0	1	1	0	1	1
		15	E	1	A	S4	S5	S6	S7	S8

C1, C2, C3, C4 - biți de control a erorilor de transmisie, deduși pe baza polinomului CRC-4.

E - biți de semnalizare a erorilor de transmisie pe baza polinomului de control CRC.

A - biți de alarmare la distanță (RAI - *Remote Alarm Indication*) care indică prin valoare logică '1', fie pierderea sincronizării, fie a unor biți de date.

S4 ... S8 - biți suplimentari sau naționali, cu semnificații specifice fiecărei țări. Dacă nu sunt utilizați, au toți valoarea logică '1'.

Observații:

1. Interfața PRI de tip E1 se configurează într-un modul software alocat acesteia, cu comenzi specifice și parametri impuși de utilizator.

2. Pentru transmisii pe linii lungi, cu interfațe PRI de tip T1, datele sunt codate folosind diverse coduri de linie bipolare:

- AMI (*Alternate Mark Inversion*) - biții '1' sunt codați alternativ prin impulsuri de polarități +/-, iar biții '0' se transmit neschimbați.
- B8ZS (*Binary Eight Zero Substitution*) - fiecare grup de opt zerouri este înlocuit cu secvența 00110011, după care se aplică legea de codare bipolară (B), cu violarea polarității (V) la fiecare al doilea bit din perechea 11, conform schemei de codare 00BV00BV.
- B7ZS (*Bipolar 7 Zero Supression*) - biții '1' se codează AMI iar fiecare al șaptelea bit '0' dintr-o secvență de 8 zerouri este înlocuit cu un bit '1' și codat prin violarea legii bipolare, respectiv prin păstrarea ultimei polarități din secvența codată.

Detalii referitoare la modul T1 de transmisie PRA se găsesc în recomandările ANSI T1.403, T1.408, T1.231 și altele.

3. În rețelele de arie largă, se utilizează sisteme de transmisie sincrone (SDH - *Synchronous Digital Hierarchy*), cu multiplexarea căilor E1 în grupuri de bandă largă, E2 de 8,192 Mbps, E3 de 32,768 Mbps și E4 de 131,072 Mbps. Similar se definesc grupurile T2, T3 și T4, de multiplexare a căilor în standardul american. Acestea sunt oferite prin serviciul ISDN de bandă largă (B-ISDN - *Broadband ISDN*).

VII.3.3 LAPD

Protocolul de acces pe canal ISDN de tip D, LAPD (*Link Access Protocol for D channel*) este un protocol de nivel OSI 2 și este descris în recomandarea ITU-T Q.921.

LAPD este utilizat în procesul de comunicație dintre TE și NT, pe nivelul legăturii de date, pentru:

- adresare;
- controlul fluxului;
- detecția erorilor de transmisie.

LAPD admite stabilirea de conexiuni logice multiple pe același canal de tip D, între echipamente de rețea de nivel OSI 3.

LAPD dispune de un modul propriu de management a conexiunilor realizate la nivelul interfețelor BRI, pentru gestionarea identificatorilor de terminal (TEI).

Din considerente de compatibilitate cu alte rețele ISDN, acest modul funcționează și în cazul interfețelor PRI deși acestea nu permit accesul multiplu.

LAPD asigură controlul apelurilor efectuate pe linie, în faza de inițiere și de încheiere a acestora, conform recomandării ITU-T Q.931 (*Q.931 Call Control*). De aceea, pe canalul D există spațiu suficient și pentru transferul unor pachete de date conform standardelor Q.931 (*Q.931 Packet Mode*) sau X.25 (*X.25 Packet Mode*).

LAPD se configurează pentru fiecare interfață BRI sau PRI, specificându-se modul de operare pe canalul D, la nivelul de rețea, prin **identificatorul de serviciu** (SAPI - *Service Access Point Identifier*) (Tabel VII.5).

Tabel VII.5

Valori SAPI tipice

SAPI	Mod de operare
0	Controlul apelului conform Q.931
1	Transfer de pachete conform Q.931
16	Transfer de pachete conform X.25
63	Management LAPD

VII.3.4 AODI

Serviciul de rețea AODI (*Always On/Demand ISDN*) realizează o conexiune permanentă între furnizorul de servicii Internet (ISP - *Internet Service Provider*) și utilizatorul unei rețele ISDN, cu transmisie de pachete pe canalul ISDN de tip D, conform standardului X.25.

Serviciul AODI nu reprezintă un protocol distinct, ci oferă o bandă de transmisie de lățime relativ mică dar și cu costuri reduse, pentru servicii de poștă-electronică, transmisii de știri în rețea și altele, eventual navigare în WWW cu creștere a benzii prin utilizarea de conexiuni pe canale B ISDN, cu circuite de comutare.

Componentele oferite de serviciul AODI sunt următoarele:

- transfer de pachete în mod X.25 pe canal D ISDN, prin conexiuni de tip 'legătură de date' (DLC - *Data Link Connection*);
- serviciu X.25 pentru protocoalele de pe nivelele OSI superioare, prin conexiuni PPP (MIOX - *Multiprotocol Interconnect Over X.25*);
- conexiuni PPP pe canalele B ISDN;
- suport pentru conexiuni PPP multiple, pe canale B și D ISDN, grupate logic într-o singură legătură PPP multiplă (*PPP Multilink Bundle*) care permite creșterea benzii disponibile pe o interfață PPP prin aplicarea protocolului de alocare a benzii (BAP - *Band Allocation Protocol*).

Interconectarea unei rețele ISDN cu o rețea TCP/IP prin intermediul serviciului AODI impune dubla identificare a fiecărui echipament (router al utilizatorului sau al ISP), atât ca adresă IP, cât și din punct de vedere la rețelei ISDN, printr-un număr ISDN alocat ISP respectiv un identificator de utilizator (TEI).

VII.4 X.25

X.25 este un standard propus inițial de CCITT, în 1976, pentru comunicația dintre un DTE (*Data Terminal Equipment*) și un DCE (*Data Circuit-terminating Equipment*) în rețele publice cu comutare de pachete (PPSN - *Public Packet Switched Network*) și completat ulterior prin recomandări ale CCITT (X.21, X.121), ISO (ISO 8208) și DDN (*Defence Data Network*) pentru realizarea de conexiuni virtuale multiple pe un singur canal fizic, pentru comunicația între mai multe DTE-uri, cu scopul creșterii eficienței de utilizare a unei legături fizice existente într-o rețea.

Comunicația dintre un DTE și DCE-ul asociat se face pe nivelul legăturii de date (*Link Layer*), pe care se menține o singură legătură permanentă din rețeaua X.25.

Conexiunile multiple, realizate în perechi de DTE-uri, se fac pe nivelele superioare, cu transfer de pachete (*Packet Layer*).

Se pot conecta la rețeaua X.25 cu comutare de pachete (XPSN - *X.25 Packet Switched Network*) ca DTE-uri, fie calculatoare individuale, fie echipamente de comunicație cu transfer de pachete PAD (*Packet Assembly/Disassembly*), de exemplu, servere de terminale sau routere, care dispun de mai multe porturi sincrone la care se conectează terminalele de date și un port sincron pentru realizarea legăturii cu rețeaua X.25 (Fig.VII.12).

Utilizatorii terminalelor de date pot apela alte DTE-uri aflate la distanță prin intermediul unui PAD. Totodată pe orice calculator se poate instala un modul software care să realizeze funcțiile specifice de PAD, acționând ca un **PAD virtual,** cu ajutorul căruia utilizatorii acelui calculator pot apela DTE-uri aflate la distanță prin intermediul unei rețele cu comutație de pachete X.25.

O rețea X.25 poate fi configurată să transporte trafic IP (*IP over X.25*) pentru realizarea unui WAN cu rutare TCP/IP.

Un router conectat la o rețea X.25 poate lucra fie ca DTE (X25T), fie ca DCE (X25C), fiind necesară pentru aceasta configurarea porturilor sale sincrone ca interfețe X.25 DTE sau X.25 DCE.

În rețeaua X.25 se utilizează două tipuri de **circuite virtuale:**

• **permanente** (PVC - *Permanent Virtual Circuit*) - configurate în DTE anterior transmisiei datelor în rețeaua X.25 și fără a necesita proceduri ulterioare de conectare sau de deconectare;

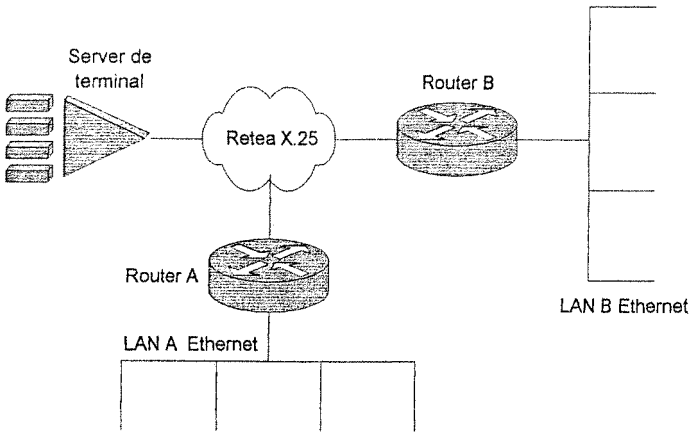


Fig.VII.12 Exemplu de interconectare a unor echipamente prin intermediul unei rețele X.25

• **comutate** (SVC - *Switched Virtual Circuit*) - create pentru fiecare apel virtual transmis în rețeaua X.25.

Un router configurat ca DCE în rețeaua X.25 utilizează numai circuite virtuale comutate (SVC).

Pe o singură legătură fizică de date, se pot crea mai multe circuite virtuale, identificate printr-un număr al canalului logic (LCN - *Logical Channel Number*). Pe o interfață X.25 se pot defini maximum 4095 de circuite virtuale (PVC sau SVC), deci se pot deschide simultan pe acea legătură de date până la 4095 de sesiuni.

Transmisia datelor printr-un circuit virtual permanent (PVC) se realizează fără întârzieri, asemănător transmisiei pe conexiuni dedicate de tip punct-la-punct.

Pentru utilizarea unui circuit virtual comutat (SVC), DTE transmite pe interfața X.25 o datagramă de tip 'cerere de apel', conținând adresa sa și cea de destinație exprimate în rețeaua X.25. Dacă DTE-ul apelat acceptă cererea, atunci se alocă un SVC și se transmit datele.

Sintaxa adresei pentru un DTE prezentată în recomandarea X.25 poate fi utilizată în orice rețea X.25 privată. Pentru rețele X.25 publice, adresarea se face conform recomandării X.121.

Adresa unui DTE dintr-o rețea X.25 constă în una până la 15 cifre din sistemul zecimal. Se pot specifica și intervale de adrese, prin înlocuirea uneia sau a mai multor cifre cu litera X.

De exemplu, un nod din rețeaua X.25 poate fi configurat să răspundă la apelul oricărui DTE care are adresa de forma 1234X. În intervalul specificat, sunt incluse zece adrese, cu valori de la 12340 la 12349.

VII.4.1 LAPB

Protocolul LAPB (*Link Access Procedure Balanced*), inclus în recomandarea X.25, se aplică pe nivelul legăturii de date folosind modul echilibrat de transmisie (*balanced mode*) specificat de protocolul HDLC.

Pentru ca un DTE sau un DCE să poată comunica prin intermediul unui port sincron, este necesară crearea la nivelul acestuia a unei interfețe logice LAPB, care să aplice procedurile specifice nivelului de legătură: control a fluxului și a erorilor de transmisie, de încapsulare a datelor în cadre fără numere de identificare etc.

Dimensiunea pachetelor care pot fi transmise printr-o interfață LAPB variază (de la 128 la 1024 de octeți).

În rețeaua X.25, pachetele sunt transmise între două DTE-uri printr-o conexiune TCP, cu diferite dimensiuni ale ferestrei de transmisie, cu confirmări de recepție corectă (ACK - *Acknowledge*) și posibilitatea de retransmisie a cadrelor în cazul apariției unor erori.

Interfața LAPB se creează și se configurează la nivelul unui port sincron al echipamentului (SYN). Această interfață devine activă abia după configurarea la nivelul ei a unei interfețe X.25 de tip DTE sau DCE, urmată de stabilirea adreselor DTE-lor în rețeaua X.25 și, eventual, configurarea unor circuite virtuale permanente (PVC).

Dacă prin intermediul rețelei X.25 se interconectează mai multe routere, configurate ca DCE-uri, atunci este necesară definirea rutelor de transmisie în rețea și asocierea adreselor din rețeaua X.25 cu adrese de nivel-rețea (de exemplu, IP).

De exemplu, se utilizează ca adresă IP a unui DTE apelat în rețeaua X.25, având o anumită adresă de tip X.25, adresa IP a routerului la care este conectat acesta.

Există câte un tabel de rutare X.25 la nivelul fiecărui router din rețea, tabel care se aplică pe toate interfețele X.25 DCE ale acestuia.

Pentru transmisia prin rețeaua X.25 a informațiilor de rutare și a altor protocoale, routerele se configurează ca DTE-uri, comunicația realizându-se fie prin PVC, fie prin SVC.

VII.4.2 ÎNCAPSULAREA DATELOR ÎN REȚEAUA X.25

Pentru transportul prin intermediul unei rețele X.25 a pachetelor create cu diferite protocoale de rețea (IP, IPX etc), se utilizează schema de încapsulare MIOX (*Multiprotocol Interconnect On X.25*), descrisă de RFC 1356.

Când o datagramă este plasată pe o interfață X.25 pentru efectuarea unui apel în rețea, se deschide la cerere un circuit virtual.

Primul octet al pachetului transmis ca cerere de apel este utilizat pentru identificarea protocolului folosit pentru încapsularea datelor transmise prin acel circuit virtual (NLPID - *Network Layer Protocol Identifier*) (Tabel VII.6).

Tabel VII.6

Valori ale NLPID folosite în rețele X.25

Valori hexazecimale ale NLPID	Protocol de încapsulare
0x.00	Protocoale multiple (încapsulare nulă)
0x.80	SNAP (*SubNetwork Address Protocol*)
0x.CC	IP
0x.EE	IPX

Încapsularea nulă (*Null Encapsulation*) se utilizează pentru multiplexarea pachetelor provenite de la mai multe protocoale de nivel rețea, pentru transmisie cu un singur circuit virtual. În acest caz, primul octet al câmpului de date din pachetul X.25 conține NLPID urmat de unitatea de date (PDU - *Protocol Data Unit*) încapsulată conform protocolului specificat.

Dacă NLPID nu este nul, atunci pentru transmisiaîn rețeaua X.25 a mai multor protocoale de rețea se stabilesc circuite virtuale multiple, câte unul pentru fiecare protocol. Câmpul de date din pachetul transmis va conține numai unitatea de date încapsulată conform unui anumit protocol.

Observație:

Dacă două routere comunică printr-un circuit X.25 MIOX cu interfețe X.25 DTE la ambele capete, atunci trebuie definit același mod de încapsulare a datelor pe ambele routere.

VII.5 TDM

Mecanismul de multiplexare în timp (TDM - *Time Division Multiplexing*) permite divizarea canalului de comunicații în mai multe intervale de timp (*time slot*) separate, care pot fi alocate mai multor utilizatori.

Acest mecanism se aplică pe interfețele ISDN de tip BRI sau PRI ale echipamentelor de comunicație din rețea.

În WAN, se utilizează diferite moduri de transmisie TDM:

- E1 TDM - oferă pe o interfață PRI o legătură statică de tip PPP (*Point-to-Point Protocol*) de 2,048 Mbps, divizată în 32 de canale de 64 kbps fiecare.
- T1 TDM - pe o interfață PRI se realizează o legătură statică PPP de 1,544 Mbps, cu 24 de canale de capacitate 64 kbps și un canal de 8 kbps rezervat pentru operații de sincronizare și întreținere a legăturii.
- BRI TDM - pe o interfață BRI se configurează static două canale de 64 kbps (B1, B2) și un canal de 16 kbps pentru informații de control.

Canalele E1/T1 TDM au fost inițial definite în sistemele telefonice digitale, pentru transmisia vocii digitizate prin metoda PCM (*Pulse Coded Modulation*) și mai precis a trunchiurilor de convorbire. Întrucât semnalul binar generat de o sursă este transparent în ceea ce privește natura informației transmise, metoda TDM s-a introdus și în rețelele WAN pentru transmisii de date.

Spre deosebire de ISDN care realizează o alocare dinamică a canalelor de comunicații, metoda TDM se aplică prin configurarea statică a echipamentelor de comunicații (bridge, router etc).

Conexiunile E1/T1 TDM admit alocarea pentru comunicația dintre două echipamente de rețea a mai multor intervale de timp (sloturi) care alcătuiesc un **grup TDM**, cu o lățime de bandă de ordinul N*64 kbps (N - numărul căilor primare care alcătuiesc grupul).

În figura VII.13, este exemplificată o schemă logică de conexiuni TDM între mai multe routere dintr-un WAN. Conform figurii, routerul A alocă 8 sloturi pentru comunicația cu routerul B, 4 sloturi pentru legătura cu routerul C și 2 sloturi pentru conexiunea cu routerul D. Similar se pot deduce căile alocate celorlalte conexiuni din rețeaua TDM.

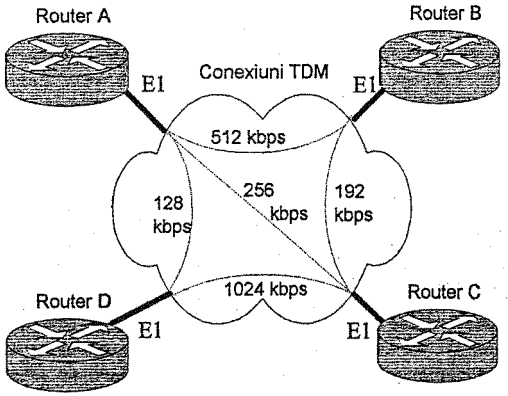


Fig. VII.13 Conexiuni TDM în WAN prin interfețe E1 TDM

Un grup TDM este echivalent cu o singură interfață fizică sincronă. Transmisia unui grup TDM se realizează pe o singură cale din WAN, printr-o singură conexiune HDLC, fără diferențiere ca în cazul ISDN când se atribuie câte o cale de transmisie fiecărui slot dintr-un grup E1/T, pe care se transmite câte un cadru HDLC. Acest fapt permite reducerea întârzierilor de transmisie diferențiale și a încărcării rețelei cu antete de cadru prin transmisie TDM, comparativ cu rețelele ISDN.

Observații:

1. Întrucât din grupul E1, slotul 0 este rezervat pentru transmisia informațiilor de încapsulare a datelor (*framing*), o conexiune E1 TDM structurată utilizează numai 31 de căi primare, deci o bandă de 1984 kbps spre deosebire de un canal E1 ISDN structurat care oferă numai 30 de canale pentru transferul datelor. Pe un canal E1 TDM nestructurat (fără divizarea fluxurilor) se transmit date în toată banda de 2,048 Mbps.

2. Pentru transmisia pe o interfață PRI ISDN în mod T1, slotul 24 este rezervat pentru semnalizări, ceea ce face ca doar 23 de sloturi să fie alocate comunicației de date. Dacă aceeași interfață este configurată ca T1 TDM, toate cele 24 de căi primare sunt utilizate pentru transferul datelor. Nu se efectuează transmisii T1 TDM în mod nestructurat.

3. O interfață PRI ISDN poate fi utilizată pentru transmisii simultane în rețele de tip ISDN și TDM, prin repartiția convenabilă a sloturilor.

4. Mecanismul TDM se poate aplica numai la un capăt al conexiunilor TDM, de exemplu pe o interfață E1, la celelalte capete fiind utilizate porturi sincrone simple, fără divizare în timp a canalului de transmisie (X.21, V.35 etc) (Fig.VII.14).

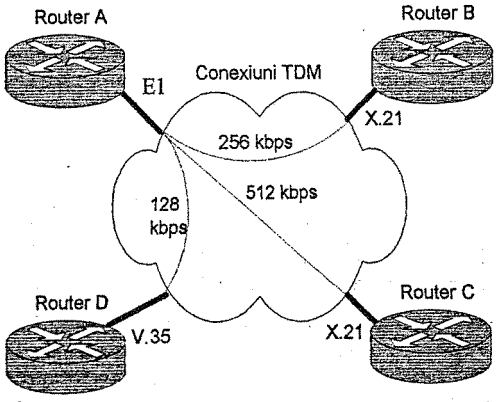


Fig. VII.14 Interconexiuni TDM în WAN cu diverse interfețe sincrone

Configurarea procedeului TDM pe un router impune:

- configurarea portului PRI pentru funcționare în regim TDM (de exemplu, E1);
- definirea grupurilor TDM;
- crearea unei interfețe PPP pentru fiecare grup TDM, prin intermediul căreia protocoalele de pe nivelele superioare comunică în WAN folosind mecanismul TDM.

VII.6 PPP

Protocolul de comunicații punct-la-punct (PPP - *Point-to-Point Protocol*) a fost dezvoltat de IETF (*Internet Engineering Task Force*) pentru standardizarea modului de transmisie a datelor cu mai multe protocoale de rețea, pe **legături seriale punct-la-punct** sincrone, ISDN, cu grupuri TDM, asincrone (ACC - *Asynchronous Communication Channel*) etc.

Protocolul PPP are trei componente principale:

- **metoda de încapsulare** a datelor în datagrame pentru transmisie pe legături seriale;
- **protocolul de control a legăturii** (LCP - *Link Control Protocol*) pentru stabilirea, configurarea și testarea conexiunilor;
- **protocoalele de control pe nivelul de rețea** (NCP - *Network Control Protocol*) pentru configurarea protocoalelor de rețea utilizate pentru transmisie.

Protocolul PPP stabilește o legătură între două noduri (puncte) din rețea printr-un scurt schimb de pachete cu opțiuni de transmisie, după care urmează transferul datelor la viteze relativ mari, în cadre nenumerotate cu puține antete, fără confirmări de recepție corectă sau retransmisii de cadre.

Interfețele logice PPP sunt create pe interfețele fizice existente (de exemplu, Ethernet). Pentru conexiuni PPP multiple, se creează mai multe interfețe PPP la nivelul unei interfețe fizice.

VII.6.1 ÎNCAPSULAREA DATELOR PRIN PPP

PPP încapsulează datele asemănător protocolului HDLC, în cadre delimitate de caractere speciale (*flags*) de un octet cu valoarea hexazecimală 7E, care se transmit și în intervalele în care nu sunt date de transmis pentru menținerea în sincronism a echipamentelor.

Cadrul PPP include, între caracterele de delimitare, mai multe câmpuri (Fig. VII.15):

- un **câmp de adresă** de un octet, cu valoarea fixă hexazecimală FF.
- un **câmp de control** de un octet, în care se înscrie valoarea hexazecimală 03, cu semnificația că se transmit cadre nenumerotate.

- un **câmp de protocol** de doi octeți, prin care se specifică tipul protocolului de rețea utilizat pentru transmisie (Tabel VII.7).
- un **câmp de date** având formatul impus de protocolul de nivel-rețea.
- un **câmp de control a erorilor de transmisie** dedus pe baza unui polinom CRC.

Câmp de delimitare 1B	Câmp de adresă 1B	Câmp de control 1B	Câmp de protocol 2B	Câmp de date max.1500 B	Câmp CRC 2B	Câmp de delimitare 1B
0x.7E	0x.FF	0x.03				0x.7E

Fig. VII.15 Formatul cadrului PPP

Pentru a evita apariția erorilor de încapsulare (*error framing*) provocate de apariția valorii caracterului de delimitare în câmpul datelor, se impune asupra șirului de date transmis constrângerea ca să nu existe mai mult de cinci biți '1' consecutivi. Cel de al șaselea bit dintr-o secvență de biți identici '1' se complementează și caracterul modificat se marchează prin transmisia anterioară acestuia a unui caracter ESC (*Escape*), corespunzător valorii ASCII hexazecimale 7D. De asemenea, orice octet de date de valoare 0x.7D este precedat de un octet identic.

Tabel VII.7

Valori și semnificații ale câmpului de protocol din cadrul PPP

Valoare	Protocol de rețea utilizat
0x.C0.21	LCP
0x.00.21	IP
0x.80.21	IPCP (*IP Control Protocol*)
0x.00.2D	TCP/IP cu compresie Van Jacobson a antetului IP
0x.00.2F	TCP/IP fără compresie
0x.00.2B	IPX
0x.80.2B	IPXCP (*IPX Control Protocol*)
0x.00.FD	Compresie de date
0x.80.FD	CCP (*Compression Control Protocol*)
0x.00.53	Criptarea datelor
0x.80.53	ECP (*Encryption Control Protocol*)
0x.00.31	*Bridging*
0x.80.31	BCP (*Bridging Control Protocol*)
0x.C0.23	PAP (*Password Authentication Protocol*)
0x.C2.23	CHAP (*Challenge Handshake Authentication Protocol*)

VII.6.2 PROTOCOALE DE CONTROL

LCP se utilizează pentru negocierea **opțiunilor de configurare** a legăturii PPP:

- unitatea maximă de date care poate fi recepționată (MRU - *Maximum Receive Unit*);
- discriminatorul de punct terminal (*Endpoint Discriminator*) - utilizat în cazul legăturilor PPP multiple (*multilink*) configurate dinamic prin PPP (RFC 1990);
- discriminatorul de legătură (*Link Discriminator*), utilizat de protocolul de alocare a benzii BAP (*Band Alocation Protocol*) pentru identificarea unei componente dintr-o legătură PPP multiplă (RFC 2125);
- protocolul de autentificare;
- raportul referitor la calitatea legăturii (LQR - *Link Quality Report*) exprimat, de exemplu, ca număr de pachete pierdute;
- "numărul magic" este o secvență de patru octeți generată aleator în procesul de negociere prin LCP și utilizată pentru identificarea și eliminarea buclelor de transmisie. Dacă pachetul LQR recepționat conține același număr magic ca cel local, atunci se consideră că a apărut o buclă în rețea și legătura este resetată.
- valorile caracterelor de control pentru transmisii asincrone (ACCM - *Asynchronous Control Character Map*);
- unitatea maximă de date care poate fi refăcută la recepție (MRRU - *Maximum Receive Reconstructed Unit*);

Apelantul transmite nodului de destinație un pachet cu opțiunile sale de configurare a conexiunii. Apelatul răspunde fie prin acceptarea opțiunilor respective, fie modificând unii parametri de configurare, fie rejectând întreg pachetul.

Faza de negociere a modului de configurare a legăturii prin PPP continuă până ce se ajunge la un acord bilateral, marcat prin transmisia unui pachet de confirmare (ACK - *Acknowledge*), după care se consideră deschisă legătura pentru comunicația prin PPP.

Urmează aplicarea procedeelor de autentificare, dacă s-a impus utilizarea lor.

Opțiunile de configurare a legăturii pentru protocoalele de nivel rețea se negociază printr-un protocol NCP (IPCP, IPXCP, CCP, ECP, BCP etc).

VII.6.3 MODALITĂȚI DE ALOCARE A BENZII

Protocolul de alocare a benzii (BAP - *Band Allocation Protocol*) se aplică pentru negocierea lățimii de bandă alocate fiecărei perechi PPP dintr-o legătură PPP multiplă (RFC 2125).

Utilizarea BAP în procesul de transmisie este posibilă numai după aplicarea protocolului de control BACP (*Band Allocation Control Protocol*) pe fiecare legătură din legătura PPP multiplă pentru negocierea opțiunii de "pereche favorită". Această opțiune permite soluționarea conflictelor de transmisie. Când două perechi PPP transmit simultan cererile BAP, perechea cu numărul magic mai mic este considerată favorită și i se alocă prioritar bandă de transmisie. BAP se configurează pe fiecare interfață PPP.

Nu întotdeauna se aplică procedeul BAP. Există și **metoda de alocare la cerere a benzii de transmisie** (*Bandwidth-on-Demand*). Procedeul este deosebit de atractiv pentru creșterea vitezei de transmisie atunci când se dispune de o conexiune pe linie închiriată care în majoritatea timpului este neutilizată sau de conexiuni ISDN multiple (Fig.VII.16). Metoda este utilă și pentru suplimentarea lățimii benzii de transmisie, precum și pentru crearea rezervelor de transmisie (*backup*) utilizabile în cazul în care legătura principală devine nefuncțională.

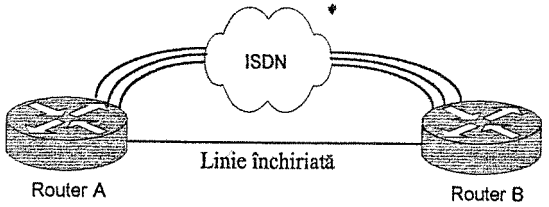


Fig. VII.16 Conexiuni PPP multiple

VII.6.4 LEGĂTURI PPP PRIN MODEMURI TELEFONICE

Interfețele PPP pentru legături sincrone pot fi configurate să controleze câte un modem telefonic conectat la rețeaua de telefonie publică (PSTN - *Public Switched Telephony Network*), pentru interconectarea ruterelor pe linie telefonică (Fig. VII.17).

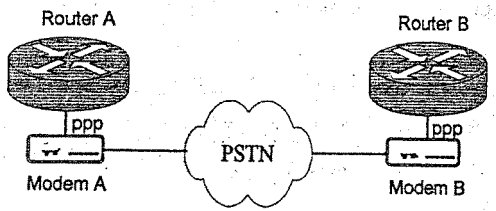


Fig. VII.17 Legături PPP cu modemuri

Controlul modemului se face prin semnalul DTR (*Data Terminal Ready*), conform satndardului V.25 bis. Pentru efectuarea unui apel sincron pe linie, routerul transmite cererea de apel telefonic (*dial-on demand*) resetând pinul DTR al modemului care a fost în prealabil configurat să apeleze un anumit număr telefonic.

Când legătura telefonică cu modemul apelat a fost stabilită, modemul apelant înștiințează routerul propriu prin intermediul semnalului DSR (*Data Set Ready*), că se poate efectua transmisia datelor.

Configurarea conexiunii dintre două routere prin intermediul unor modemuri telefonice se face mai lent decât în cazul unei rețele ISDN.

În plus, există riscul apariției unei coliziuni atunci când routerele se apelează simultan. În acest caz, după 15 secunde ambele apeluri sunt anulate, urmând a fi reluate după intervale de timp cu durate stabilite pe baza unui algoritm de aleatorizare.

VII.7 TEHNOLOGII xDSL

O linie digitală de abonat (DSL - *Digital Subscriber Line*) constă într-o pereche de modemuri interconectate printr-o linie telefonică, în particular un cablu torsadat în pereche, cu conductoare din cupru.

Transmisia pe o astfel de linie se face în mod duplex, cu viteze de ordinul a 160 kbps, la distanțe maxime de circa 5,6 km fără repetoare, folosind banda de frecvențe [0 ... 80] kHz.

Tehnologiile xDSL permit transferul datelor pe linia telefonică la viteze foarte mari, prin folosirea unor tehnici avansate de modulații digitale cu număr mare de stări (QAM - *Quadrature Amplitude Modulation*; TCM - *Trellis Coded Modulation* etc), a tehnicilor de compresie a datelor și de corecție a erorilor de transmisie, precum și a unor coduri de linie adecvate (Manchester; CMI - *Coded Mark Inversion*; AMI - *Alternate Mark Inversion*; HDBn - *High Density Bipolar n* etc):

- HDSL (*High-Data rate Digital Subscriber Line*) - transmite pe linie un canal E1 de 2,048 Mbps sau T1 de 1,544 Mbps, la distanțe de circa 3,7 km fără repetoare.
- SDSL (*Single-line Digital Subscriber Line*) - este o variantă a HDSL, cu transmisie pe o singură pereche de fire, la distanțe de cel mult 3 km. Poate fi utilizată în rețeaua telefonică clasică.
- ADSL (*Asymmetric Digital Subscriber Line*) - este creată pentru aplicații multimedia, transmisii video la cerere, acces la Internet sau într-o rețea locală aflată la distanță etc.

Tehnologia ADSL oferă viteze foarte mari de transmisie a datelor pe linia telefonică.

Se folosesc două canale de transmisie a datelor, unul spre client (*downstream*), altul spre furnizorul de servicii (*upstream*), **dimensionate asimetric.** De exemplu, pentru transmisia unui

film în format MPEG se utilizează un canal de până la 3 Mbps spre client și unul de ieșire de maximum 64 kbps, cu un raport de asimetrie de circa 50:1. Pentru navigare în Internet, raportul lățimilor de bandă a celor două canale este de ordinul 10:1. Dimensionarea corespunzătoare a celor două canale din sistemul ADSL permite transmisia datelor spre client la viteze foarte mari, cu valori ce depind de lungimea segmentului de cablu (Tabel VII.8).

Tabel VII.8

Vitezele și distanțele maxime de transmisie în sisteme ADSL, în funcție de dimensiunile cablului utilizat

Viteza de transmisie (Mbps)	Diametrul conductoarelor (mm)	Distanța maximă de transmisie (km)
1,544/2,048	0,5	5,5
1,544/2,048	0,4	4,6
6,192	0,5	3,7
6,192	0,4	2,7

Observații:

1. Limitarea distanței maxime de transmisie, respectiv a segmentului de cablu, este cauzată de atenuările specifice cablurilor din sistemele de comunicație și de încărcarea capacitivă maximă admisă de echipamentele folosite.

2. Unele limitări ale vitezei de transmisie a datelor prin intermediul rețelei telefonice sunt determinate de partea de transport a acesteia (*network core*).

ANEXA A

ALGORITMI DE REȚEA

Pentru reprezentarea grafică a unei rețele de calculatoare se folosește **metoda grafurilor.**

Nodurile grafului simbolizează calculatoarele sau, mai general, echipamentele terminale de date (DTE), respectiv echipamentele de comunicație de date (DCE).

Legăturile fizice existente în rețea sunt reprezentate în graf prin **săgeți** cu o singură orientare în cazul transmisiei simplex sau cu dublu sens pentru comunicațiile duplex.

Descrierea funcționării rețelei este realizată prin **diagrame cu număr finit de stări,** cărora li se asociază algoritmi de procesare specifici. Aceștia se implementează fie ca procese în cadrul sistemului de operare, fie ca programe software independente activate odată cu sistemul de operare. Se pot utiliza diferite limbaje de programare pentru scrierea acestora.

Prin intermediul algoritmilor de rețea, se realizează controlul traficului de pachete la nivelul nodurilor, al congestiilor și eventual al jetonului de acordare a permisiunii de transmisie.

Apar aspecte distincte în funcționarea unei rețele centralizate, respectiv a uneia descentralizate (Fig. A.1 a; b).

Graful (a) de **rețea centralizată** (Fig.A-1a) cuprinde un nod central (M - *master*) care supervizează activitatea întregii rețele, în sensul că orice mesaj se transmite prin intermediul acestui nod, chiar dacă transmisia se face între două noduri subordonate (*slave*), de exemplu S_k și S_j. Nodul M constituie astfel un controler de rețea. Defectarea acestuia afectează funcționarea întregii rețele.

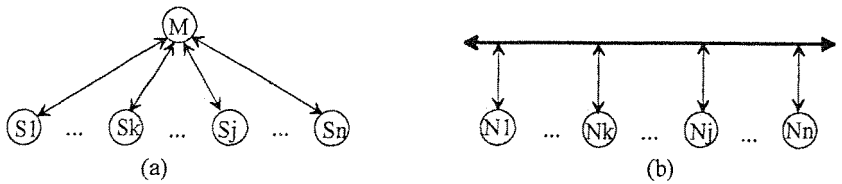


Fig. A.1 Grafuri de rețea: (a) centralizată; (b) descentralizată.

De exemplu, în nodul M poate fi amplasat un *hub* care să controleze accesul la mediu al stațiilor din nodurile *slave* printr-o topologie logică de tip 'stea' (*star*).

În graful asociat unei **rețele descentralizate** (Fig. A-1b), toate nodurile au drepturi egale în rețea, fiecare nod fiind responsabil de controlul traficului de pachete la nivelul său. Într-o rețea cu topologie fizică de tip 'magistrală' (*bus*), accesul la mediu se poate face fie prin metoda CSMA/CD, fie prin cea cu jeton, *token-passing*. Defectarea unui nod nu le afectează pe celelalte.

A.1 Algoritmul nodului *master*

Nodul central M (*master*) adresează în ordine cererea de transmisie fiecărui nod din rețea (S_j). Dacă acesta are un mesaj de transmis, se realizează transmisia lui din nodul S_j către M și stocarea sa în memorie. Expedierea lui către nodul-destinație se va face atunci când se va stabili comunicația cu nodul respectiv (S_k). **Algoritmul nodului *master*** se repetă pe toată durata funcționării rețelei, deservind periodic toate stațiile din rețea.

În figura A.2, se prezintă o schemă logică pentru algoritmul nodului *master*.

O variantă de implementare a acestui algoritm în limbaj C este prezentată în continuare:

```
repeat
      k:=1
      repeat
            if(mesaj pentru nodul Sk) then
                  trimite mesajul nodului Sk;
            endif
            adreseaza cererea de transmisie nodului Sk;
            if(mesaj de transmis din nodul Sk) then
                  acorda permisiunea de transmisie nodului Sk;
                  accepta mesajul din nodul Sk;
            endif
```



```
            k:=k+1
      until k:=n+1 (*n - numarul total de noduri slave din retea *)
until se intrerupe functionarea.
```

În cazul apariției unui defect la nivelul nodului central, toate comunicațiile dintre nodurile rețelei sunt afectate. Acest dezavantaj nu apare în rețelele descentralizate, care au astfel o mai mare siguranță și flexibilitate în funcționare.

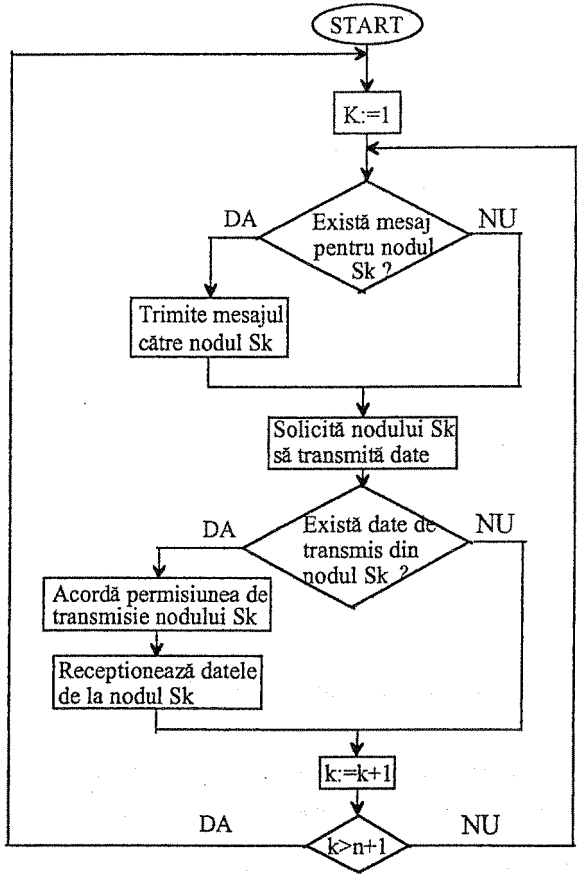


Fig. A.2 Algoritmul nodului MASTER

A.2 Algoritmul unui nod *slave*

Un nod *slave* subordonat celui coordonator central, *master*, se găsește în **starea de așteptare** atâta timp cât nu i se trimit pachete și nu este solicitat să transmită.

Nodul devine **activ** în momentul în care se recepționează un cadru dinspre nodul *master*. Se decide dacă acesta reprezintă un mesaj destinat nodului *slave* sau este un cadru de control de tip 'solicitare de transmisie'. Urmează în funcție de caz, fie recepționarea datelor, fie trimiterea către nodul *master* a cererii pentru acordarea permisiunii de transmisie, dacă există date de transmis și dacă modul de acces la mediu se bazează pe utilizarea 'jetonului de transmisie'.

În figura A.3, se prezintă un exemplu de algoritm pentru nodul *slave*. Algoritmul este rulat ciclic până la întreruperea funcționării nodului respectiv. Eventuala blocare a nodului într-una din stări se poate soluționa prin resetarea acestuia și reinițializarea algoritmului.

Un model de scriere a acestui algoritm în limbaj C este prezentat mai jos.

```
repeat
      asteapta mesaj dinspre nodul master;
      if(mesaj destinat nodului slave) then
            accepta mesajul transmis de nodul master;
      elseif(solicitare de transmisie) then
            if(exista date de transmis) then
                  cere permisiunea de transmisie;
                  asteapta acordarea permisiunii de transmisie;
                  transmite datele catre nodul master;
            endif
      endif
until se intrerupe functionarea nodului.
```

A.3 Algoritmul unui nod dintr-o rețea descentralizată

Într-o rețea descentralizată (Fig. A.1b), toate nodurile au aceeași prioritate.

Modul de ocupare a canalului de comunicații se bazează fie pe metoda de ascultare a canalului pentru a identifica momentul în care acesta este liber pentru transmisie, cu riscul apariției unor coliziuni între pachetele transmise simultan pe aceeași cale, fie pe metoda 'jetonului' pentru evitarea blocajelor de trafic.

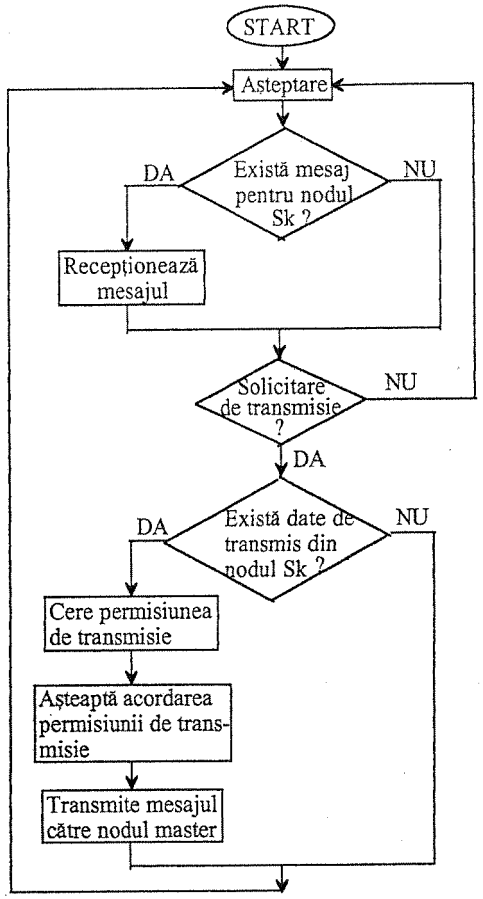


Fig. A.3 Algoritmul nodului SLAVE

Rețelele Ethernet sunt LAN-uri descentralizate CSMA/CD.

Algoritmul pentru un nod N_k dintr-o rețea descentralizată, cu 'jeton de transmisie', este prezentat în figura A.4. Acesta este rulat ciclic până la întreruperea funcționării nodului.

Implementarea algoritmului în limbaj C se poate face ca în următorul model:

```
repeat
      asteapta primirea unui cadru;
      if(mesaj pentru nodul Nk) then
```

```
            receptioneaza mesajul;
      elseif(jeton) then
            if(exista mesaj de transmis din nodul Nk) then
                  transmite mesajul;
            endif
            transmite jetonul nodului urmator;
      endif
until se intrerupe functionarea nodului.
```

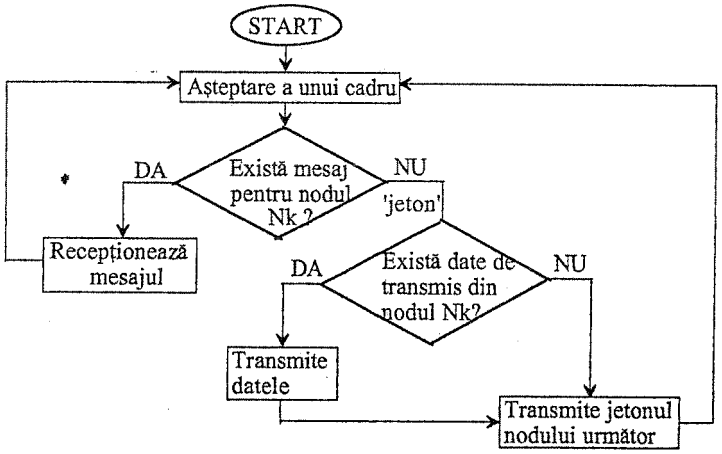


Fig.A.4 Algoritmul unui nod Nk
dintr-o rețea descentralizată

A.4 Algoritmul CSMA/CD

Tehnica CSMA/CD presupune că nodurile rețelei sunt într-o permanentă concurență pentru obținerea dreptului de utilizare a mediului fizic de transmisie. Nodul care ocupă rețeaua la un anumit moment transmite un singur pachet după care este obligat să elibereze canalul. În timp ce unul din noduri transmite, toate celelalte sunt în așteptare. Dacă mai multe noduri încearcă să transmită simultan, atunci apare o coliziune între pachete.

În figura A.5 sunt reprezentate grafic două situații specifice, într-o topologie fizică de tip ' magistrală' (*bus*).

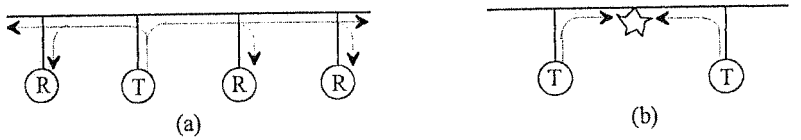


Fig.A.5 Transmisie în rețea 'bus': (a) broadcast; (b) cu coliziune.

Nodurile notate T sunt în starea de transmisie, iar cele notate R recepționează date.

În primul caz (Fig.A-5a), un singur nod transmite către toate celelalte noduri ale rețelei (*broadcast*).

În cazul (b), se observă apariția unei coliziuni cauzată de transmisii simultane efectuate de două noduri din rețea. Semnalele transmise interferă ceea ce conduce la distorsionarea lor și imposibilitatea recuperării datelor, adică pierderea mesajelor.

În această situație, fiecare nod își oprește procesul de transmisie și trece într-o stare de inactivitate (*back-off*), cu durata stabilită pe baza unui generator de secvență aleatoare (*jamming*). Este important ca duratele acestei stări, pentru nodurile implicate în coliziune să aibă durate diferite astfel încât nodurile să nu încerce retransmisia simultan, ceea ce ar conduce la apariția unei noi coliziuni și eventual propagarea fenomenului la infinit. Durata acestei stări poate fi stabilită proporțional cu adresa nodului ceea ce elimină riscul repetării coliziunii, dar introduce o anumită ierarhie de priorități în rețea, întrucât întotdeauna nodul cu adresă de valoare mai mică va ocupa mai repede canalul de comunicație și va transmite datele înaintea unui nod cu o adresă de valoare mai mare.

Schema de aplicare a metodei CSMA/CD rulează în fiecare nod la nivelul legăturii de date, pe baza diagramei de stări prezentate în figura A.6.

La punerea în funcțiune sau după resetarea nodului, acesta se află în **starea inițială** de testare sau "ascultare" a mediului de transmisie.

Dacă are de transmis date, atunci nodul trece în **starea de așteptare** până când se eliberează canalul și începe **transmisia**. Aceasta poate să decurgă normal, caz în care după finalizarea transmisiei nodul revine în starea inițială, sau este posibil să apară o coliziune ceea ce determină oprirea procesului de transmisie și obligarea nodului la **inactivitate** pentru o anumită perioadă de timp, după care intră din nou în starea de așteptare pentru a retransmite cadrul.

Din starea inițială, este posibil ca un cadru transmis să fie destinat nodului, adică în câmpul adresei de destinație să apară chiar adresa nodului respectiv (MID - *"My IDentifier"*). Alte noduri ignoră cadrul respectiv dar nodul căruia îi este adresat îl **acceptă** și începe recepția. Dacă aceasta decurge normal, la final nodul va reveni în starea inițială.

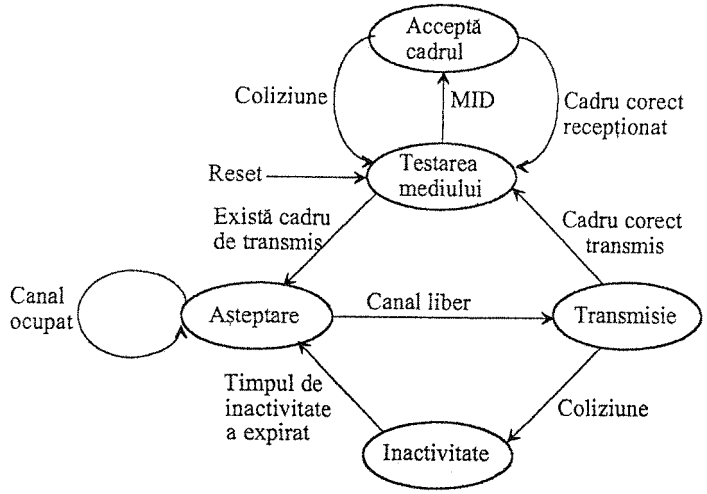


Fig.A.6 Algoritmul CSMA/CD

Dacă apar coliziuni pe durata recepției, nu se confirmă recepția cadrului (NAK - *Not Acknowledge*) și nodul trece în starea de ascultare a canalului. Nodul-sursă va retransmite cadrul respectiv.

A.5 ALGORITMUL TOKEN-BUS

Evitarea apariției coliziunilor într-o rețea locală este posibilă prin utilizarea 'jetonului de acordare a permisiunii de transmisie'.

Inițial rețeaua trebuie configurată pentru a stabili ordinea în care jetonul este transmis de la o stație la alta.

În arhitectura token-bus, terminalele sunt conectate logic în inel ceea ce presupune că fiecare nod din rețea cunoaște propria adresă (MID) și adresa următorului nod (NID - *Next IDentifier*) căruia îi va pasa jetonul. Acest proces de învățare la nivelul fiecărui nod a NID se realizează prin algoritmul de 'votare' (*polling*) care se va încheia în momentul în care se închide inelul logic și toate adresele nodurilor sunt incluse în inelul logic. În figura A.7, este prezentată spre exemplificare o rețea token-bus. Stația 5 nu este în funcțiune și, prin urmare, nu este inclusă în inelul logic.

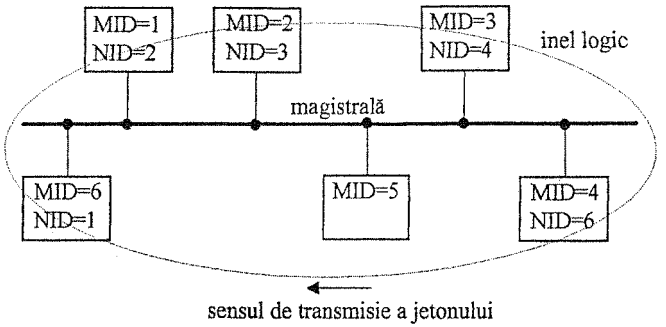


Fig.A.7 Exemplu de rețea Token-Bus

Evident, dacă un nou terminal se conectează la rețea, este necesară reconfigurarea acesteia pentru includerea noului nod în lista de adrese. Aceasta presupune întreruperea procesului normal de funcționare printr-un procedeu de bruiaj (*jamming*) care determină pierderea jetonului și lansează algoritmul de regăsire a acestuia (*token-recovery*).

Inițial toate nodurile se găsesc în starea de "somn", adică sunt inactive pe o durată de timp proporțională cu adresa sau ID-ul fiecăreia. În această stare se ajunge și prin lansarea în rețea a semnalului de bruiaj de către un terminal care dorește să se conecteze la inelul logic. Evident, nodul cu adresa minimă va fi primul activ și va începe procesul de 'votare'. Acesta trimite jetonul pe magistrala de date și așteaptă răspuns din partea următoarei stații, în ordine crescătoare a adreselor. Noua stație va ieși din starea de inactivitate la primirea jetonului și va continua procesul de 'votare'. Stațiile care au determinat NID-ul, intră în procesul normal de funcționare, conform algoritmului token-bus (Fig.A.8). Dacă în rețea este activă o singură stație, nu se poate forma inelul logic și acel terminal rămâne în starea de așteptare până la intrarea în funcțiune a altor stații.

A.6 ALGORITMUL TOKEN-RING

Spre deosebire de rețeaua de tip token-bus, rețeaua token-ring utilizează un inel fizic, ceea ce presupune că transmiterea unui pachet între două noduri neadiacente se face prin intermediul altor noduri.

Coliziunile sunt evitate prin folosirea jetonului de transmisie dar într-o rețea token-ring acesta poate fi 'liber' sau 'ocupat'. Evident, o stație poate transmite date doar dacă primește jetonul liber.

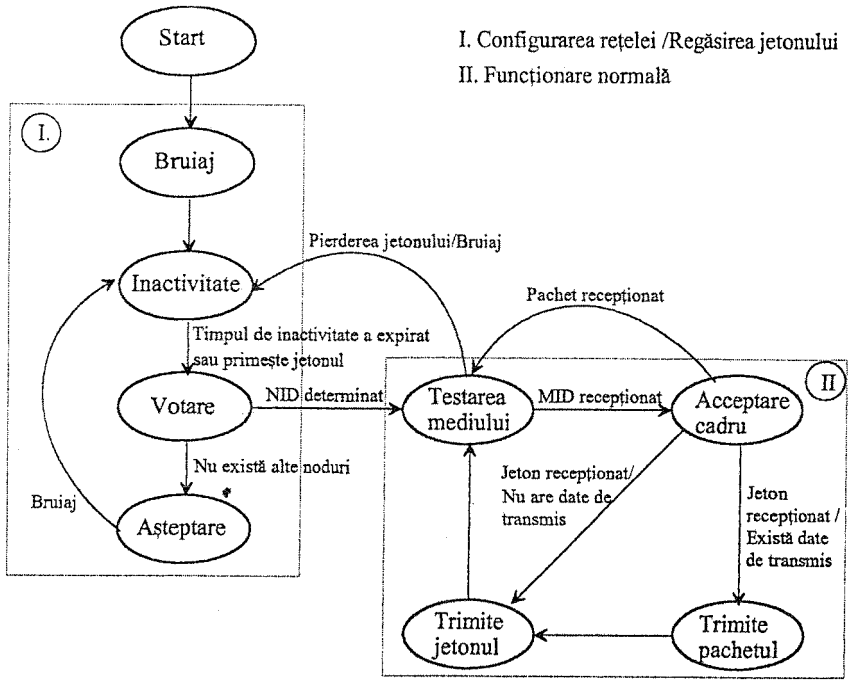


Fig. A.8 Algoritmul Token-Bus

Jetonul este 'ocupat' atunci când precede un pachet de date, urmând a fi eliberat de nodul care a expediat pachetul.

Jetonul liber circulă între stații, pe inelul fizic, în ordinea conectării acestora la inel.

În figura A.9, este prezentată ca exemplu o rețea token-ring cu 4 stații.

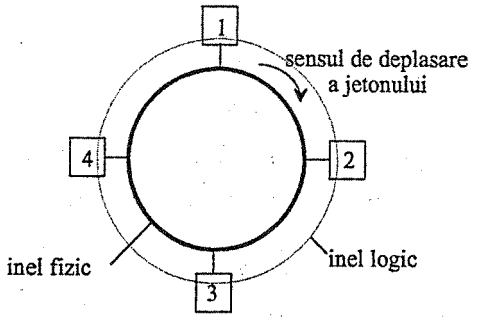


Fig.A.9 Exemplu de rețea în inel

Inițial jetonul circulă liber până când una din stații are mesaj de transmis și devine activă. Să presupunem că stația 1 deține jetonul și trimite un pachet către stația 3. Forma jetonului se modifică pentru a indica starea de 'ocupat' a acestuia pe durata transportării pachetului. Cadrul transmis de stația 1, conținând jetonul 'ocupat' și datele, ajunge la stația 2. Presupunem că și stația 2 are de transmis date. Întrucât jetonul este ocupat, aceasta va rămâne în așteptare și va realiza doar transferul cadrului de la stația 1 către stația 3. Stația 3 își recunoaște adresa (ID) și preia datele dar nu eliberează jetonul ci îl transmite mai departe ca 'ocupat'pe inel împreună cu confirmarea de primire corectă a pachetului (ACK) către stația 1 prin intermediul nodului 4. Stația 1 recepționează pachetul și eliberează jetonul. Jetonul 'liber' ajunge la stația 2 care va putea transmite. Pe durata transmisiei efectuate de un nod, toate celelalte noduri sunt pasive, adică realizează doar transferul pachetului către următorul nod (*forwarding*).

Algoritmul Token-Ring este prezentat în figura A.10.

Apar modificări față de acest algoritm în situația transformării rețelei token-ring în rețea star-ring.

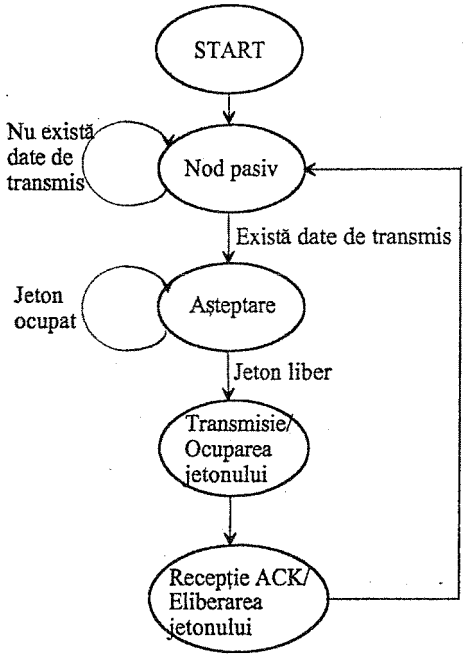


Fig. A.10 Algoritmul Token-Ring

APLICAȚIE

Scrieți în limbaj C următorii algoritmi de rețea:

a. CSMA/CD.

b. "de votare" (*polling*).

c. Token-Bus cu funcționare normală.

d. Token-Bus pentru configurarea rețelei.

e. Token-Ring.

ANEXA B

COMENZI UNIX UZUALE

B.1 GENERALITĂȚI

Sistemul UNIX lucrează în mod linie de comandă.

Accesarea unui sistem UNIX se face pe baza **numelui de utilizator** și a **parolei**:

login: nume_utilizator <Enter>

password:

Parola va avea minimum șase caractere alfanumerice, cu minimum două alfabetice și minimum unul nealfabetic în primele șase.

După introducerea corectă a acestora și validarea lor, apare **prompterul de sistem**:

$ pentru Bourne Shell și Korn Shell

% pentru C Shell

pentru contul administratorului de sistem.

Shell-ul emite prompterul și interpretează comenzile.

Prima fază de interpretare a unei comenzi în sistemul UNIX constă în recunoașterea numelui comenzii sau generarea unui mesaj de eroare referitor de sintaxă incorectă.

Shell-urile Bourne și Korn admit introducerea comenzilor pe mai multe linii, caz în care pe următoarele linii apare prompterul: >.

Unele comenzi UNIX acceptă exprimarea unor opțiuni și introducerea de argumente (caractere, nume de fișiere sau de directoare), respectând sintaxa:

$ comanda [- optiuni] [argumente] <Enter>

Separarea elementelor din linia de comandă se face cu unul sau mai multe spații libere și/sau tab-uri.

Opțiunile sunt precedate de o cratimă (-).

Dacă se exprimă mai multe comenzi pe aceeași linie, acestea se separă prin 'punct-și-virgulă' (;). Se pot introduce comenzi în timpul execuției alteia, fiecare păstrîndu-se în memorie până ce se termină executarea celei precedente.

Observații

1. Combinația dintre o tastă și tasta CTRL se va nota cu simbolul ^ urmat de acel caracter.
2. Ștergerea caracterelor se face cu tasta *BackSpace* sau ^H.
3. Oprirea din execuție a programului curent se face acționând ^C care determină afișarea prompterului.
4. Întreruperea tuturor proceselor aflate în execuție (*kill*) se face prin comanda ^U. Se poate defini alte secvențe pentru diferite porcese dorite, folosind comanda:

stty [-optiuni] [argumente]

stty -a	afișează toate caracteristicile terminalului.
stty proces "secventa"	definește tasta sau combinația de taste care determină executarea unui proces.

Exemplul 1. Pentru aflarea datei și a orei, se introduce comanda:

$ date <Enter>

Această comandă acceptă exprimarea unor opțiuni și argumente referitoare la formatul de afișare (%d.%m.%Y, %H:%M:%S).

Exemplul 2. Pentru ieșirea din sistem, se dă comanda:

$ exit <Enter>

sau

$ <CTRL-d>

Exemplul 3. Schimbarea parolei proprii se face cu comanda:

$ passwd <Enter>

Exemplul 4. Definirea secvenței (Ctrl-H) de ștergere a caracterelor, se face cu comanda:

$ stty erase "^H" <Enter>

Exemplul 5. Secvența (Ctrl-c) de întrerupere a execuției unui program, se definește astfel:

$ stty intr "^C" <Enter>

Exemplul 6. Comanda de afișare a unui mesaj pe ecran are obligatoriu ca argumente șirul de caractere care vor fi reprezentate, eventual încadrate cu apostroafe dacă lungimea mesajului depășește lungimea liniei de pe ecran:

$ banner ' BINE ATI <Enter>
> VENIT' <Enter>

Se observă apariția prompterului > pentru continuarea liniei anterioare.

Alte comenzi cu caracter general sunt:

who	comanda de aflare a informațiilor despre utilizatorii activi la un moment dat.
who am i	afișează numele utilizatorului și informații despre terminal.
whoami	afișează numai numele utilizatorului activ la acel moment, pe terminal.
man [-k|n] termen	afișează informațiile conținute în manualul de sistem, referitoare la un cuvânt sau o comandă specificată în argumentul "termen", cu opțiunea -k pentru afișa toate intrările ce conțin acel termen, sau cu specificarea numărului secțiunii dorite din manual (n).
whereis termen	comanda de deducere a secțiunilor care fac referiri la termenul dorit.
mail	comanda de citire a mesajelor din căsuța poștală proprie.
mail [destinatar]	comanda de expediere a unui mesaj prin sistemul de poștă electronică (Expedierea este marcată de combinația de taste ^d).
write [destinatar]	comandă de scriere către un alt utilizator, activ la același calculator.
mesg [y|n]	comanda de acordare sau invalidare a permisiunii de scriere la acel terminal (fără opțiuni, afișează setarea anterioară).

Observații:

- Tasta <Space> determină afișarea următoarei pagini cu informații utile.
- Tasta <Enter> permite afișarea următoarei linii.
- Cu tasta <q> (*Quit*) se iese din manual.

- Afișarea mesajelor se face pe principiul LIFO (*Last-In First-Out*).
- Comanda mail își introduce propriul prompter (?) care poate fi urmat de una din următoarele comenzi:

?	se solicită informații ajutătoare (*help*).
d	șterge mesajul afișat din cutia poștală (*delete*).
s [fisier]	salvează mesajul în fișierul specificat (*save*).
<Enter>	determină afișarea următorului mesaj.
+	idem.
-	afișează mesajul anterior.
![comanda]	execută o altă comandă UNIX.
q	ieșire din cutia-poștală cu eventuale modificări (*quit*).
x	ieșire din cutia-poștală fără a schimba conținutul acesteia (*exit*).

B.2 ORGANIZAREA SISTEMULUI DE FIȘIERE SUB UNIX

Sistemul de fișiere într-un sistem UNIX este organizat ierarhic, sub forma unei diagrame de tip 'arbore', cu un nod-rădăcină (notat: /), cu directoare, subdirectoare și fișiere (Fig.B.1).

Pe primul nivel se găsesc următoarele directoare:

/bin	conține fișierele de execuție a comenzilor pentru operațiile de bază în sistemul de operare și manipulare de fișiere.
/dev	conține driverele componentelor hardware din sistem.
/etc	cuprinde programele accesibile numai administratorului de sistem.
/ux	reprezintă directorul-sistem, care conține sistemul de operare UNIX.
/usr	include comenzi uzuale, altele față de cele incluse în directorul /bin.
/tmp	conține fișiere temporare.
/users	include subdirectoarele de lucru și conturile utilizatorilor.

Structura se ramifică în subdirectoare:

/usr/bin	cuprinde comenzi suplimentare, care nu sunt absolut necesare sistemului.
/usr/mail	include ca subdirectoare "cutiile poștale" (*mailboxes*) ale utilizatorilor.
/usr/local/bin	conține aplicațiile dezvoltate local.
/usr/man	reprezintă manualul cu informații ajutătoare pentru utilizatori.
/users/user1	este directorul creat de către administrator pentru utilizatorul 1.
/users/user2	este directorul creat de către administrator pentru utilizatorul 2 ș.a.m.d.

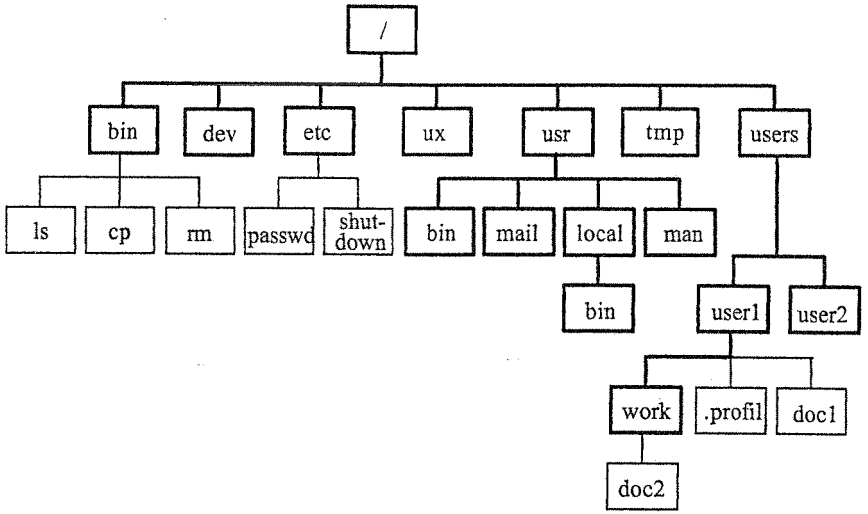


Fig.B.1 Structură de sistem de fișiere sub UNIX

Observație:

La crearea unui director, se definesc automat două directoare, notate "." și "..", pentru exprimarea simplificată a căilor relative în graf:

.	reprezintă directorul curent.
..	semnifică nodul ierarhic superior, adică directorul "părinte".

Exemplul 7. Din nodul "user1" se definesc următoarele căi cu semnificațiile specificate:

.	echivalent cu	/users/user1
..	echivalent cu	/users
../..	echivalent cu	/
./work	echivalent cu	/users/user1/work
../user2	echivalent cu	/users/user2
../../usr	echivalent cu	/usr

B.3 COMENZI DE OPERARE CU DIRECTOARELE

pwd	comanda de determinare a directorului curent (*present working directory*), exprimă calea absolută din graf spre directorul curent.

cd [director] comanda de schimbare a directorului curent (*change directory*) în cel exprimat în mod relativ sau absolut ca argument al comenzii. Fără argumente, determină întoarcerea în directorul de login (*home directory*).

mkdir [-p] [director] comandă de creare a directorului (***make directory***), eventual a celor intermediare dacă nu există (se include opțiunea -p). E admisă crearea simultană a mai multor directoare. Se exprimă ca argument fie calea absolută, fie una relativă pentru fiecare director nou creat.

rmdir [director] comandă de ștergere a directorului (***remove directory***) cu condiția să nu conțină fișiere sau subdirectoare. E admisă ștergerea simultană a mai multor directoare.

ls [optiuni] [cale] comanda de listare (***list***) a directoarelor și fișierelor subordonate nodului exprimat prin argumentul "cale", relativ sau absolut. Opțiuni:

- -a listează toate (*all*) subdirectoarele și fișierele, inclusiv cele de configurare, cu prefixul "."
- -d listează caracteristicile directorului.
- -l listează atributele tuturor fișierelor incluse în director.
- -F listează formatat conținutul directorului (se specifică sufixul / în cazul subdirectoarelor și sufixul * pentru fișierele executabile).
- -R listează recursiv toate fișierele din directorul curent și din subdirectoarele subordonate acestuia.

Observație:

Unele sisteme UNIX admit folosirea comenzilor sub formă prescurtată. Orice comandă se execută numai după acționarea tastei <Enter>.

Exemplul 8. Comanda de listare formatată a directoarelor și fișierelor subordonate nodului 'rădăcină' se dă sub forma:

```
$ ls -F<Enter>
```

sau

```
$ lsf <Enter>
```

Exemplul 9. Se aplică aceste comenzi pentru nodul "User2". Observați efectele lor.

```
$ pwd
```



```
/users/user2
$ ls .. /user1
work        doc1
$ ls -aF /users/user1
work/       .profil     doc1
$ ls ..
user1       user2
$ ls -F ..
user1/      user2/
$ ls -R ..
user1       user2
./user1:
work        doc1
$ ls user1
user1 not found
$ cd ..
$ pwd
/users
$ cd ..
/
$ cd ..
/
$ cd /usr
$ pwd
/usr
$ ls -F .
bin/        mail/       local/      man/
$ mkdir  proba
$ pwd
/usr
$ cd ./proba
$ mkdir dir1  dir2
$ ls -F
```

```
dir1/          dir2/
$ cd ..
$ rmdir proba
rmdir: proba not empty
$ rmdir        proba/dir1    proba/dir2    proba
$ cd ../bin
$ ls -F
ls*    cp*    rm*
```

B.4 COMENZI DE OPERARE CU FIȘIERELE

Prin **fișier** (*file*) se înțelege o colecție de date, de natură diversă: text, imagine, driver, executabil, director.

Cu un editor de texte, se introduc caractere ASCII și se obține un **fișier obișnuit** (*regular file*).

Dacă se scrie un program folosind un limbaj de programare (C++, Turbo C, Java) se obține un cod-sursă care prin compilare devine **fișier executabil** (*program file*), stocat într-un director de tip /bin.

Mai multe fișiere sunt stocate într-un **director** (*directory*), care reprezintă un fișier special, conținând numele și adresele de memorie ale componentelor, precum și numerele de identificare ale acestora în sistemul de fișiere (*inode number*).

Pentru componentele hardware se folosesc fișiere de tip 'driver', de interfațare cu sistemul de operare (*kernel*), denumite și **fișiere periferice** (*device file*), stocate în directorul /dev.

Numele fișierului are maximum 255 de caractere alfanumerice și de punctuație: 'punct' (.), cratimă' (-), 'liniuță de subliniere' (_). În unele variante de UNIX această limită are valori mai mici, de exemplu, 14 în HP-UX.

Ca răspuns la comanda ls -l, **tipul** fișierului se specifică pe prima poziție, astfel:

- \- fișier obișnuit
- d director
- l fișier de legătură
- n fișier de rețea
- c driver pentru un periferic de afișare a caracterelor
- b driver pentru un periferic care lucrează cu blocuri de date

- p driver pentru un canal de comunicație interprocese (*pipeline*).

Ca atribute ale unui fișier se mai specifică, în afară de tipul acestuia, drepturile de acces (citire, scriere), număr de noduri subordonate, nodul ierarhic superior, dimensiunea fișierului exprimată în octeți, data și ora când a fost accesat ultima oară și în final, numele fișierului.

Afișarea pe ecran a conținutului unui fișier se poate face fie în întregime, prin comanda cat, având obligatoriu ca argiment numele fișierului, fie segmentat, pagină cu pagină, folosind comanda more.

Dacă se dorește **afișarea ultimelor n linii** dintr-un fișier, atunci se dă comanda:

tail [-n] [nume fisier]

Alte comenzi de operare cu fișierele sunt următoarele.

Comanda de copiere:

cp [-optiuni] [fisier1] [director|fisier2]

Se copie fisierul 1 într-un nou fișier 2, creat în același director dacă nu se precizează alt director, sau într-un fișier cu același nume (fisier1) dar în directorul specificat de cel de-al doilea argument al comenzii, eventual sub un alt nume (fisier2) dacă este dat în comandă.

Primul argument poate fi multiplu, cu condiția ca destinația să fie un director.

Opțiunile comenzii pot fi:

- \- i de operare interactivă, pentru a se cere acordul în cazul suprascrierii unui fișier deja existent.
- -r de operare recursivă, în cazul în care dorim să copiem în întregime un director în alt director.

Mutarea sau redenumirea unui fișier (director) se face cu comanda:

mv [-optiuni] [director|fisier1] [director|fisier2]

Și în acest caz, ca argumente se folosesc căi absolute sau relative ale unor fișiere sau directoare.

Opțiunea de operare interactivă - i ne avertizează în cazul în care există deja la destinație un fișier cu același nume ce urmează a fi rescris.

Comanda de mutare a fișierelor diferă de cea de copiere prin faptul că nu se creează fișiere noi, numărul total de fișiere nu se modifică.

Comanda de ștergere a unui fișier sau a conținutului unui director este:

rm [-optiuni] [director|fisier]

În acest caz, este indicată folosirea opțiunii de operare interactivă - i .

Ştergerea tuturor fişierelor dintr-un director este posibilă prin includerea în linia de comandă a opţiunii de operare recursivă - r, fiind recomandată exprimarea ambelor opţiuni - ir. Spre deosebire de comanda rmdir în acest caz, directorul există în continuare, dar nu mai conţine nimic.

Opţiunea - f determină ştergerea necondiţionată, fără avertismente a tuturor fişierelor specificate în lista de argumente.

Exemplul 10. Se consideră nodul curent user1. Observaţi efectele următoarelor comenzi:

```
$ pwd
/users/user1
$ ls -F
work/          doc1
$ ls work
doc2
$ cp doc1 work
$ ls  work
doc1 doc2
$ cp doc1 doc3
$ ls -F
work/          doc1          doc3
$ cat doc1
Acesta este un fisier de test.
Se foloseste pentru exemplificarea comenzilor.
$ cat doc3
Acesta este un fisier de test.
Se foloseste pentru exemplificarea comenzilor.
$ tail -1 doc3
Se foloseste pentru exemplificarea comenzilor.
$ ls .. /user2
ls: user2 is empty
$ cp doc1 doc3 .. /user2
$ ls .. /user2
doc1 doc3
```



```
$ cp -ri work .. /user2
$ cd .. /user2
$ ls -FR
work/          doc1          doc3
./work:
doc1           doc2
$ mv doc3 work
$ ls -F
work/          doc1
$ ls work
doc1           doc2          doc3
$ mv work  test
$ ls -F
test/          doc1
$ ls test
doc1           doc2          doc3
$ rm -i  doc1
doc1? y
$ cat doc1
cat: cannot open doc1
$ ls -F
test/
$ rm  test
rm: test directory
$ rm -r test
$ ls test
test is empty
$ ls -F
test/
$ rmdir test
$ ls
user2 is empty
$ cd ..
```

```
$ mv user1 user2
$ ls user1
user1 is empty
$ ls user2
work        doc1
```

Observație:

În cazul operării interactive, utilizatorul poate răspunde afirmativ, tastând y (*yes*), ori negativ, prin n (*no*) sau <Enter>.

ABREVIERI

1000 Base CX *Dual-Coaxial Cable 1000Mbps Ethernet*
1000 Base LX *Fiber 1000 Mbps Ethernet (1270 nm)*
1000 Base SX *Single Mode Fiber 1000 Mbps Ethernet (830 nm)*
1000 Base TX *Unshielded Twisted-Pair 1000 Mbps Ethernet*
100 Base-FX *Fiber Fast Ethernet Network*
100 Base-TX *Unshielded Twisted Pair Fast Ethernet*
10 Base 2 *Thin Ethernet*
10 Base 5 *Thick Ethernet (StarLAN 10)*
10 Base F *Fiber Ethernet*
10 Base T *Unshielded Twisted-Pair 10 Mbps Ethernet*
1Base5 *(StarLAN) Unshielded Twisted Pair 1 Mbps Ethernet*
3DES *Triple Data Encryption System*
4B5B *4 - to -5 Bit Coding*

A

AAL *ATM Adaptation Layer*
AC *Access Control*
ACC *Asynchronous Communication Channel*
ACCM *Asynchronous Control Character Map*
ACELP *Adaptive Code Excited Linear Prediction*
ACGN *Additive Coloured Gaussian Noise*
ACK *ACKnowledge*
ACL *Access Control List*
ACU *Automatic Calling Unit*
ADPCM *Adaptive Differential Pulse Coded Modulation*
ADSL *Asymmetric Digital Subscriber Line*
AGP *Advanced Graphics Card*
AH *IP Authentication Header*
AIS *Alarm Indication Signal*
AM *Amplitude Modulation*
AMI *Alternative Mark Inversion*

ANSI	*American National Standards Institute*
AODI	*Always On/Demand ISDN*
AP	*Application Processor/ Access Point*
APDU	*Application Protocol Data Unit*
API	*Application Program Interface*
APK	*Amplitude-Phase Keying*
ARP	*Address Resolution Protocol*
ARPA	*Advanced Research Project Agency*
AS	*Autonomous System*
ASCII	*American Standard Code for Information Interchange*
ASK	*Amplitude Shift Keying*
ASN	*Autonomous System Number*
ATM	*Asynchronous Transfer Mode*
AU	*Attachment Unit*
AUI	*Attachment Unit Interface*
AWGN	*Additive White Gaussian Noise*

B

b	*bit*
B	*Byte*
B7ZS	*Bipolar 7 Zero Supression*
B8ZS	*Binary Eight Zero Substitution*
BACP	*Band Allocation Control Protocol*
BAP	*Band Allocation Protocol*
BATE	*Baseband Adaptive Transversal Equalizer*
BB	*Base Band*
BCD	*Binary Coded Decimal*
BCP	*Bridging Control Protocol*
BECN	*Backward Explicit Congestion Notification*
BEL	*Bell*
BGP	*Border Gateway Protocol*
BIP-L	*BIPhase-Level*
BIOS	*Basic Input-Output System*
B-ISDN	*Broadband ISDN*
BOOTP	*BOOTstrap Protocol*
BOP	*Byte Oriented Protocol*
BNC	*Bayonet Nut Connector*
bps	*bits-per-second*
BPSK	*Binary Phase Shift Keying*
BR	*Bridge-Router*
BRA	*Basic Rate Access*
BRI	*Basic Rate Interface*
BS	*BackSpace*
BSA	*Basic Service Area*
BSC	*Basic Station Controller*
BSS	*Basic Service Set*
BSD-UX	*Berkeley Software Distribution Unix*
BTC	*Basic Transceiver*
BUS	*Broadcast Unknown Server*

C

CBAC	*Context-Based Access Control*
CBR	*Constant Bit Rate*
CCITT	*International Consultative Committee for Telephony and Telegraphy*
CCP	*Compression Control Protocol*
CD	*Carrier Detect*
CDDI	*Copper Distributed Data Interface*
CDE	*Common Desktop Environment*
CDFS	*Compact Disk File System*
CDMA	*Code Division Multiple Access*
CELP	*Code Excited Linear Prediction*
CE-QAM	*Constant Envelope Quadrature Amplitude Modulation*
CES	*Circuit Emulation Service*
CLP	*Cell Loss Priority*
CHAP	*Challenge Handshake Authentication Protocol*
CIDR	*Classless InterDomain Routing*
CIR	*Committed Information Rate*
CISC	*Complet Instruction Set Computing*
CLLM	*Consolidated Link Layer Management*
CMI	*Coded Mark Inversion*
CMOS	*Complementary Metal Oxid Semiconductor*
C/N	*Carrier-to-Noise Ratio*
CODEC	*COder-DECoder*
CP	*Communication Processor*
CPCS	*Common Part Convergence Sublayer*
CPFSK	*Continuous Phase Frequency Shift Keying*
CPU	*Central Processing Unit*
CR	*Carriage Return*
CRC	*Cyclic Redundancy Checking*
CS	*Checksum / Card Services / Convergence Sublayer*
CSMA/CA	*Carrier Sense Multiple Access with Collision Avoidance*
CSMA/CD	*Carrier Sense Multiple Access with Collision Detection*
CSS	*Card and Socket Specification*
CTS	*Clear-To-Send*
CU	*Central Unit*

D

DA	*Destination Address*
DAS	*Dual Attachment Station*
DCE	*Data Circuit Terminal Equipment / Distributed Computing Environment*
DDN	*Defence Data Network*
DEC	*Digital Equipment Corporation*
DES	*Data Encryption System*
DHCP	*Dynamic Host Configuration Protocol*
DIR	*Desired Information Rate*
DLC	*Data Link Control / Data Link Connection*
DLCI	*Data Link Connection Identifier*

DLL	*Dynamic Link Library*
DNS	*Domain Name System*
DOS	*Disk Operating System*
DPMA	*Demand Priority Media Access*
DPP	*Demand Priority Protocol*
DPSK	*Differentially Phase Shift Keying*
DS	*Distribution System*
DSAP	*Destination Service Access Point*
DSB-AM	*Double Side Band Amplitude Modulation*
DSL	*Digital Subscriber Line*
DSP	*Digital Signal Processing*
DSR	*Data Set Ready*
DSSS	*Direct Sequence Spread Spectrum*
DTE	*Data Terminal Equipment*
DTMF	*Dual Tone MultiFrequency*
DTR	*Data Terminal Ready*
DVMRP	*Distance Vector Multicast Routing Protocol*

E

EBCDIC	*Extended Binary Coded Decimal Interchange Code*
ECP	*Encryption Control Protocol*
ED	*Ending Delimiter*
EGP	*Enhanced Gateway Protocol*
EGRP	*Enhanced IGRP*
EIA	*Electronics Industries Association*
EISA	*Extended Industry Standard Architecture*
E-mail	*Electronic mail*
EMI	*ElectroMagnetic Interference*
ENAT	*Enhanced Network Address Translation*
ENCO	*ENcryption & COmpression*
ENQ	*ENQuire*
ESA	*Extended Service Area*
ESS	*Extended Service Set*
ESP	*IP Encapsulating Security Payload*
ETH	*Ethernet*

F

FAQ	*Frequently Asked Questions*
FAT	*File Allocation Table*
FC	*Fragment Control / Frame Control*
FCS	*Frame Check Sequence*
FDDI	*Fiber Distributed Data Interface*
FDMA	*Frequency Division Multiple Access*
FEC	*Forward Error Correction*
FF	*Form Feed*
FHSS	*Frequency Hopping Spread Spectrum*
FIFO	*First-In First-Out*

FIN	*Final flag*
Finger	*Finger User-information Protocol*
FI	*Fragment Identification*
FM	*Frequency Modulation*
FR	*Frame Relay*
FS	*File System / Frame Status*
FTP	*File Transfer Protocol / Foil Twisted Pair*

G

Gbps	*Giga bits-per-second*
GbE	*Gigabit Ethernet*
GF	*Galois Field*
GFC	*General Flow Control*
GIF	*Graphic Interchange Format*
GMSK	*Generalised Minimum Shift Keying*
GRE	*Generic Routing Encapsulation*
GUI	*Graphic Unit Interface*

H

H	*Header / Host*
HAL	*Hardware Abstraction Layer*
HDBn	*High Density Bipolar Code no.n*
HDD	*Hard-Disk Drive*
HDLC	*High-level Data Link Control*
HDSL	*High-Data Rate Digital Subscriber Line*
HEC	*Header Error-Control*
HL, HLEN	*Header Length*
HPFS	*High-Performance File System*
HP-UX	*Hewlett-Packard Unix*
HT	*Horizontal Tab*
HTML	*HyperText Markup Language*
HTTP	*HyperText Transfer Protocol*

I

IANA	*Internet Assigned Number Agency*
IBSS	*Independent Basic Service Set*
ICMP	*Internet Control Message Protocol*
ID	*IDentifier*
IEEE	*Institute of Electrical and Electronic Engineers*
IER	*Interrupt Enable Register*
IETF	*Internet Engineering Task Force*
IGMP	*Internet Group Management Protocol*
IGRP	*Internal Gateway Routing Protocol*
IIR	*Interrupt Identifier Register*
IKE	*Internet Key Exchange*

InterNIC	*Internet Network Information Center*
Intranet	*Internal Local Web Servers*
I/O	*Input/Output*
IP	*Internet Protocol*
IPCP	*Internet Protocol Control Protocol*
I-P-O	*Input-Processing-Output*
IPng	*IP next generation*
IPsec	*Internet Protocol Security Facility*
IPX	*Internetwork Packet eXchange*
IPXCP	*Internetwork Packet eXchange Control Protocol*
IRDA	*InfraRed Data Access*
IRQ	*Interrupt ReQuest*
ISA	*Industry Standard Architecture*
ISAKMP	*Internet Security Association and Key Management Protocol*
ISDN	*Integrated Services Digital Network*
ISI	*InterSymbol Interference*
ISO	*International Standards Organisation*
ISOC	*Internet SOCiety*
Iso-Ethernet	*Isochronous Ethernet*
ISP	*Internet Service Provider*
ISTE	*Integrated Services Terminal Equipment*
ITU	*International Telecommunication Union*
IWF	*Interworking Function*

J

JPEG	*Joint Photographic Experts Group*

K

kbps	*kilo bits-per-second*

L

LAN	*Local Area Network*
LAPB	*Link Access Procedure Balanced*
LAPD	*Link Access Protocol for D-channel*
LCN	*Logical Channel Number*
LCP	*Link Control Protocol*
LES	*LAN Emulation Server*
LF	*Line Feed*
LLC	*Logical Link Control*
LMI	*Local Management Interface*
LPC	*Local Procedure Call*
LQR	*Link Quality Report*
LST	*Link State Technology*
LT	*Line Termination*

M

Mbps	*Mega bits-per-second*
MA	*Multiple Access*
MAC	*Media Access Control / MiniAccelerator Card*
MAN	*Metropolitan Area Network*
Manchester	*Biphase-L Coding*
MAU	*Multistation Access Unit*
MCA	*Micro Channel Architecture*
MCR	*Modem Control Register*
MFT	*Master File Table*
MG	*Media Gateway*
MGCP	*Media Gateway Control Protocol*
MIB	*Management Information Base*
MID	*My IDentifier*
MII	*Media Independent Interface*
MIME	*Multipurpose Internet Mail Extension*
MIOX	*Multiprotocol Interconnect Over X.25*
MLID	*MultiLink Interface Driver*
MMF	*MultiMode Fiber*
MNP	*Microcom Networking Protocol*
MODEM	*MOdulator DEModulator*
MPEG	*Movie Photographic Experts Group*
MPLS	*MultiProtocol Label Switching*
MRC	*MultiRate Coder*
MRRU	*Maximum Receive Reconstructed Unit*
MRU	*Maximum Received Unit*
MS-DOS	*Microsoft Disk Operating System*
MSB	*Most Significant Bit*
MSC	*Mobile Switching Center*
MSK	*Minimum Shift Keying*
MSR	*Modem Status Register*
MTA	*Message Transfer Agent*
MTU	*Maximum Transmission Unit*

N

NAK	*Not AcKnowledge*
NAT	*Network Address Translation*
NAV	*Network Allocation Vector*
NBF	*NetBEUI Frame*
NCB	*Network Control Block*
NCP	*Netware Core Protocol / Network Control Protocol*
NDIS	*Network Driver Interface Specification*
NetBeui	*Network BIOS extended user interface*
NetBIOS	*Network Basic Input/Output System*
NFS	*Network File System*
NIC	*Network Interface Card*
NID	*Next IDentifier*

NLPID	*Network Layer Protocol IDentifier*
NOS	*Network Operating System*
NMM	*Network Management Module*
NMS	*Network Management Station*
NNI	*Network - Network Interface*
NPM	*Network Protocol Module*
NT	*Network Termination*
NTFS	*NT File System*
NTP	*Network Time Protocol*
NUL	*Null*
NVT	*Network Virtual Terminal*

O

ODI	*Open Data-link Interface*
OFDM	*Orthogonal Frequency Duplexing Method*
ONC	*Open Network Computing*
OQPSK	*Offset Quadrature Phase Shift Keying*
OS	*Operating System*
OSI	*Open Systems Interconnection*
OSPF	*Open Shortest Path First*
OUI	*Organizational Unique Identifier*

P

PAD	*Packet Assembly/Disassemby*
PAP	*Password Authentication Protocol*
PBX	*Public Branche eXchange*
PC	*Personal Computer*
PCI	*Peripheral Component Interconnect*
PCM	*Pulse Coded Modulation*
PCMCIA	*Personal Computer Memory Card International Association*
PDU	*Protocol Data Unit*
PERL	*Practical Extraction and Reporting Language*
PG	*Protective Ground*
PGP	*Pretty Good Privacy*
PI	*Protocol Interpreter*
PING	*Packet InterNetwork Groper*
PMD	*Physical Medium Dependent*
PMP	*Point - to - Multipoint*
PnP	*Plug and Play*
POP	*Post-Office Protocol*
PP	*Point-to-Point*
PPDU	*Presentation Protocol Data Unit*
PPP	*Point-to-Point Protocol*
PPSN	*Public Packet Switched Network*
PRA	*Primary Rate Access*
PRI	*Primary Rate Interface*
PS	*Postscript*

PSK	*Phase Shift Keying*
PSH	*Push flag*
PSTN	*Public Switched Telephony Network*
PSU	*Power Supply Unit*
PTY	*Payload TYpe*
PVC	*Permanent Virtual Circuit*

Q

QAM	*Quadrature Amplitude Modulation*
QoS	*Quality of Service*
QPRS	*Quadrature Partial Response Signal*
QPSK	*Quadrature Phase Shift Keying*

R

RADIUS	*Remote Authentication Dial In User Service*
RAI	*Remote Alarm Indication*
RAM	*Random Access Memory*
RARP	*Reverse Address Resolution Protocol*
RAS	*Remote Access Service*
RFI	*Radio Frequency Interference*
RJ	*Registered Jack*
RFC	*Request For Comments*
RFI	*Radio Frequency Interference*
RIP	*Routing Information Protocol*
RISC	*Reduced Instruction Set Computing*
RLL	*Run-Length Limited*
RLP	*Resource Locator Protocol*
RMON	*Remote Monitoring*
PnP	*Plug-n-Play*
ROM	*Read-Only Memory*
RPC	*Remote Procedure Call*
RST	*Reset flag*
RSVP	*ReSerVation Protocol*
RTCP	*Real Time Control Protocol*
RTF	*Rich Text Format*
RTP	*Real Time Protocol*
RTS	*Request-To-Send*
RxD	*Data Receiving*

S

SA	*Source Address / Security Association*
SAM	*Security Account Manager*
SAP	*Service Access Point / Service Advertising Protocol*
SAPI	*Service Access Point Identifier*
SAR	*Segmentation And Reassemble*

SAS	*Single Attachment Station*
SCO	*Santa Cruz Operation*
SCSI	*Small Computer System Interface*
ScTP	*Screened Twisted Pair*
SD	*Starting Delimiter*
SDH	*Synchronous Digital Hierarchy*
SDLC	*Synchronous Data Link Control*
SDSL	*Single-line Digital Subscriber Line*
SEAL	*Simple Efficient Adaptation Layer*
SFTP	*Simple File Transfer Protocol*
SFSK	*Sinusoidal Frequency Shift Keying*
SG	*Signal Ground / Signaling Gateway*
SLIP	*Serial Line Internet Protocol*
SMB	*Server Message Block*
SMF	*Single-Mode Fiber*
SMI	*Structure of Management Information*
SMP	*Symmetric Multiprocessing*
SMTP	*Simple Mail Transfer Protocol*
SN	*Sequence Number*
SNA	*Service Network Architecture*
SNAP	*SubNetwork Access Protocol*
SNMP	*Simple Network Management Protocol*
SNR	*Signal-to-Noise Ratio*
SNTP	*Simple Network Time Protocol*
SPAP	*Shiva Password Authentication Protocol*
SPD	*Security Policy Database*
SPDU	*Session Protocol Data Unit*
SPI	*Service Parameter Index*
SPX	*Sequenced Packet eXchange*
SRM	*Security Reference Monitor*
SS	*Socket Services / Spread Spectrum*
SS-7	*Signaling System no.7*
SSAP	*Source Service Access Point*
SSCS	*Service Specific Convergence Sublayer*
SSH	*Secure SHell Protocol*
STA	*Station Adapter / Spanning-Tree Algorithm*
STP	*Shielded Twisted Pair*
SVC	*Switched Virtual Circuit*
SVR4-UX	*At&T System V Release 4 Unix*
SYN	*Synchronize flag*

T

Tbps	*Tera bits-per-second*
TA	*Terminal Adapter*
TC	*Transmission Convergence*
TCL	*Tool Command Language*
TCM	*Trellis Coded Modulation*
TCP	*Transmission Control Protocol*
TCP/IP	*Transport Control Protocol/Internet Protocol*

TDM	*Time Division Multiplexing*
TDMA	*Time Division Multiple Access*
TE	*Terminal Equipment*
TEI	*Terminal Endpoint Identifier*
Telnet	*Virtual Terminal Connection*
TFM	*Tamed Frequency Modulation*
TFTP	*Trivial File Transport Protocol*
TIA	*Telecommunication Industry Association*
TIME	*Time of Day Protocol*
ToS	*Type of Service*
TL	*Total Length*
TPDU	*Transport Protocol Data Unit*
TSAPI	*Telephony Services Application Programmable Interface*
TSM	*Telephony Signaling Module*
TTL	*Time-To-Live*
TTY	*TeleTYpe*
TxD	*Data Transmission*

U

UA	*User Agent*
UART	*Universal Asynchronous Receiver- Transmitter*
UDP	*User Datagram Protocol*
UNI	*User-Network Interface*
UPS	*Uninterruptible Power Supply*
URG	*Urgent flag*
URI	*Uniform Resource Identifier*
URL	*Uniform Resource Locator*
URN	*Uniform Resource Name*
USB	*Universal Serial Bus*
UTP	*Unshielded Twisted Pair*
UUCP	*Unix-to-Unix Copy Program*

V

VBR	*Variable Bit Rate*
VCI	*Virtual Channel Identifier*
V/FoIP	*Voice/Fax-over-IP*
VPI	*Virtual path Identifier*
VLAN	*Virtual Local Area Network*
VoATM	*Voice-over-ATM*
VoDSL	*Voice-over-Digital Subscriber Line*
VoFR	*Voice-over-Frame Relay*
VoIP	*Voice-over-IP*
VoN	*Voice-over-Network*
VoP	*Voice-over-Packet*
VPM	*Voice Packet Module*
VPN	*Virtual Private Network*
VSB	*Vestigial Side Band*

VT	*Virtual Terminal / Vertical Tab*
VxD	*Virtual Device Driver*

W

WAN	*Wide Area Network*
WDMA	*Wavelength Division Multiple Access*
WFQ	*Weighted Fairly Queuing*
WINS	*Windows Internet Name Service*
WLAN	*Wireless Local Area Network*
WM	*Wireless Medium*
WWW	*World Wide Web*

X

XNS	*Xerox Network Standard*
XPSN	*X.25 Packet Switched Network*

BIBLIOGRAFIE

[1] BLACK U.D. *TCP/IP and Related Protocols*, McGraw-Hill, 1995

[2] BERTSEKAS D., GALLAGER R. *Data Networks*, Prentice-Hill, 1992

[3] CHELLIS J., PERKINS C., STREBE M. *MCSE: Networking Essentials*, SYBEX Inc., Alameda, 1998

[4] COMER D.E. *The Internet Book*, Prentice-Hall, 1995

[5] DE PRYCKER M. *Asynchronous Transfer Mode*, Ellis Horwood, 1993

[6] HANDLEY M., CROWCROFT J. *The World Wide Web - Beneath the Surf*, London UCL Press 1994

[7] HUITEMA C. *Routing in the Internet*, Prentice-Hall, 1995

[8] IEEE 802.3 *Carrier Sense Multiple Action with Collision Detection*, New York IEEE 1985a

[9] IEEE 802.4 *Token Passing Bus Access Method*, New York IEEE 1985b

[10] IEEE 802.5 *Token Ring Access Method*, New York IEEE 1985c

[11] JAMSA K., COPE K. *Internet Programming*, Jamsa Press, 1995

[12] KAUFMAN C., PERLMAN R., SPECINER M. *Network Security*, Prentice Hall, 1995

[13] KESSLER G.C. *ISDN*, McGraw-Hill, 1993

[14] PERLMAN R. *Interconnections: Bridges and Routers*, Addison-Wesley, 1992

[15] PISCITELLO D.M., CHAPIN A.L. *Open Systems Networking: TCP/IP and OSI*, Addison - Wesley, 1993

[16] SMITH P. *Frame Relay*, Addison - Wesley, 1993

[17] TANENBAUM A.S. *Modern Operating Systems*, Prentice Hall, 1992

[18] TANENBAUM A. S. *Computer Networks*, Prentice-Hall, 1996

[19] TOLMIE D.E. *Gigabit Networking*, IEEE LTS, vol.3, 1992

*** Documente RFC accesibile în WWW